Digitale Zertifikate im Bildungsbereich unter besonderer Berücksichtigung von öffentlichen Bildungsanbietern

Bachelorarbeit

Im Studiengang Bibliothekswissenschaft

Vorgelegt von

Daniel Lubszczyk

TH Koeln

Institut für Informationswissenschaft

Technology
Arts Sciences
TH Köln

Abstract

Mit dem Fortschritt und der Verbreitung neuer Technologien findet auch im Bildungsbereich eine zunehmende Digitalisierung statt. Ein bisher der Digitalisierung gegenüber resistenter Bereich von Bildung waren analoge Zertifikate. Aufgrund der fortbestehenden Probleme von analogen Zertifikaten hat sich dieser Trend geändert. Aktuell experimentieren verschiedene Bildungsanbieter mit unterschiedlichen Modellen, um Alternativen zu analogen Zertifikaten zu finden.

Die vorliegende Arbeit beschreibt anhand von unterschiedlichen Beispielen digitale Zertifikate und untersucht – unter besonderer Beachtung des Bildungsauftrags von öffentlichen Bildungsanbietern –, inwiefern digitale Zertifikate geeignet sind, analoge Zertifikate zu ersetzen. Die Zielgruppe der Arbeit sind öffentliche Bildungsanbieter, die momentan analoge Zertifikate ausstellen. Die Ergebnisse der Arbeit sind allerdings für alle Bildungsanbieter relevant.

Aus den Stärken, Schwächen und sonstigen Eigenschaften von analogen Zertifikaten sowie aus den sich aus dem öffentlichen Bildungsauftrag für Bildungsanbieter ergebenden Werten wird ein idealtypischer Kriterienkatalog erstellt. Die verschiedenen digitalen Zertifikate werden in einer SWOT-Analyse mithilfe der erstellten Kriterien untersucht und verglichen.

Das Ergebnis der Untersuchung ist, dass zwei verschiedene Ansätze von digitalen Zertifikaten existieren. Einerseits gibt es digitale Zertifikate, die analoge Zertifikate zu ergänzen versuchen, und andererseits digitale Zertifikate, die analoge Zertifikate vollkommen zu ersetzen versuchen.

Momentan erfüllen digitale Zertifikate des Self-Sovereign-Identity-Types den Kriterienkatalog am besten. Die Untersuchung zeigt allerdings, dass alle Arten von digitalen Zertifikaten eigene Stärken besitzen und Lösungen zu den aktuellen Problemen von analogen Zertifikaten bieten. Deswegen sollten andere Types nicht unmittelbar verworfen werden.

Stichworte: Blockchain, Zeugnis, Zertifikat, Bildung, Self-Sovereign Identity

Along the progress and spread of new technology education also experiences an increasing digitalization. An area so far resistant to digitalization was analogue certificates. Based on the ongoing problems of analogue certificates however, this trend has changed. Currently different education providers are experimenting with different models to find alternatives to analogue certificates.

This work describes digital certificates using different examples and investigates, considering the educational task of public education providers, how digital certificates are suitable to replace analogue certificates. This work is aimed at public education providers that currently issue analogue certificates. The results are relevant for all education providers.

Based on the strengths, weaknesses and characteristics of analogue certificates, as well as the resulting values based on the educational task of public education providers, an ideal-typical catalogue of criteria is created. The different types of digital certificates are analyzed and compared to each other with a SWOT analysis, relying on the previously created criteria.

The results of this investigation show that there are two different approaches to digital certificates. On one hand there are digital certificates that try to complement analogue certificates and on the other hand there are digital certificates that aim to completely replace analogue certificates.

Currently digital certificates of the Self-Sovereign Identity type fulfill the criteria catalogue the best. Though the investigation shows, that all types of digital certificates possess their own strengths and provide solutions to the problem analogue certificates are currently facing. For this reason other types should not be discarded.

Keywords: Blockchain, Certificate, Education, Self-Sovereign Identity

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Ausstellen von Zertifikaten stellt eine essenzielle Aufgabe jeder öffentlichen Bildungseinrichtung dar, deren Umsetzung bislang größtenteils analog erfolgt. Im Gegensatz dazu laufen Prozesse wie Bewerbungsverfahren inzwischen vermehrt digital ab. Ausgehend von diesem Trend und aktuellen Problemen von analogen Zertifikaten, wird erkennbar, dass im Bildungsbereich Alternativen zu analogen Zertifikaten benötigt werden. Um diese Alternativen zu ermitteln und in ihrer Relevanz zu beurteilen wurde die Forschungsfrage aufgestellt: „Welche Formen digitaler Zertifikation können zukünftig die analoge Zertifikation im Bildungsbereich ersetzen?“.

Ziel der Arbeit ist es, einen Überblick von aktuellen digitalen Zertifikaten zu erstellen und herauszuarbeiten, unter welchen Rahmenbedingungen die verschiedenen Arten von digitalen Zertifikaten am besten genutzt werden können. Die Ausgangsthese „Digitale Zertifikate des Self-Sovereign-Identity-Types werden (in den nächsten fünf bis zehn Jahren) die am weitesten verbreitete Alternative zu analogen Zertifikaten im Bildungsbereich sein.“ wird mithilfe eines Kriterienkatalogs und einer SWOT-Analyse anhand von Beispielen überprüft. Das Ergebnis der Arbeit soll den Lesern – hauptsächlich Entscheidungsträger bei öffentlichen Bildungsanbietern – ermöglichen, eine eigene, auf Fakten basierende Strategie zum Umstieg auf digitale Zertifikate zu entwickeln.

Im zweiten Kapitel werden grundlegende Bestandteile und Komponenten von Zertifikaten sowie charakterisierende Eigenschaften und aktuelle Probleme von analogen Zertifikaten im Bildungsbereich vorgestellt. Das zweite Kapitel erläutert das nötige Grundwissen über analoge Zertifikate und beinhaltet den ersten Teil an Informationen, die später zur Beurteilung von digitalen Zertifikaten im Kontrast zu analogen Zertifikaten genutzt werden.

Im dritten Kapitel wird die Einschränkung der Forschungsfrage auf öffentliche Bildungsanbieter erläutert. Im Kontrast zu anderen Gruppen von Bildungsanbietern haben öffentliche Bildungsanbieter im öffentlichen Bildungsauftrag eine große Gemeinsamkeit. Diese grenzt sie klar von kommerziellen Bildungsanbietern ab.

Im vierten Kapitel wird die genutzte Typologie von digitalen Zertifikaten beschrieben. Jeder Type wird anhand von Beispielen und Schaubildern erläutert. Ziel dieses Kapitels ist es, dem Leser zu ermöglichen, den Type derjenigen digitalen Zertifikate, die in der Arbeit nicht als Beispiele genutzt werden, selbstständig zu erkennen.

Im fünften Kapitel wird zunächst ein Kriterienkatalog für digitale Zertifikate aus den zusammengetragenen Informationen und Eigenschaften analoger Zertifikate sowie aus der besonderen Perspektive von öffentlichen Bildungsanbietern erstellt. Mithilfe der erstellten Kriterien werden die verschiedenen Types in einer SWOT-Analyse untersucht. Der Kriterienkatalog und die SWOT-Analyse werden als Methoden genutzt, um Fairness und Vergleichbarkeit in der Untersuchung von digitalen Zertifikaten zu erreichen. Abschließend werden die Ergebnisse dieser Untersuchung, angeordnet nach den verschiedenen Kriterien, verglichen. Die Ergebnisse dieses Vergleichs werden am Ende des Kapitels in einer Tabelle zusammengefasst.

Abschließend wird das Fazit der vorliegenden Arbeit gezogen und ein Ausblick auf die Zukunft von Zertifikaten im öffentlichen Bildungsbereich entworfen.

2 Analoge Zertifikation

Aktuelle analoge Zertifikate im Bildungsbereich werden genutzt, um vertrauenswerte Aussagen über die Identität und Vergangenheit einer Person zu machen.[1] Zertifikate bestehen aus verschiedenen Komponenten und mehreren beteiligten Personen oder Organisationen:

1. Die Behauptung[2]
2. Der Aussteller[3]
3. Die Beweise[4]
4. Der Empfänger[5]
5. Das Zertifikat[6]
6. Die Signatur[7]
7. Dritte[8]

Bei der Behauptung handelt es sich um eine Aussage, die das Zertifikat beglaubigen soll. Beispielsweise „der Schüler hat eine spezifische Fertigkeit erlangt“ oder „dieser Lehrer darf Schüler unterrichten“.[9]

Der nächste Teil eines Zertifikats ist der Aussteller. Meistens ist dieser eine Organisation oder eine Person, die im Namen einer Organisation handelt. Der Aussteller überprüft Fakten und sagt aus, dass die Behauptung wahr ist.[10] Ein Beispiel für einen Aussteller ist die TH Köln, eine öffentliche Fachhochschule.

Die folgende Komponente sind Beweise, die die Behauptung unterstützen. Meistens gehören hierzu sowohl die Prozedur, wie die Behauptung überprüft wurde, als auch Informationen über die Behauptung an sich. Beispielsweise wird beim Erlangen eines ECTS-Punktes mit dem Zertifikat eine ECTS-Anleitung und -Erklärung, wie die Prozedur zum Erlangen dieses Punktes funktioniert hat, mitgeliefert.[11]

Die nächste involvierte Person ist der Empfänger, der Adressat. Der Empfänger erhält meistens auch das Zertifikat oder eine Kopie desselben.[12] Beispiele für Empfänger sind Studenten und Schüler.

---

[1] Grech 2017: *Blockchain in Education*, S. 27.
[2] ebd.
[3] ebd.
[4] ebd.
[5] ebd.
[6] ebd.
[7] ebd.
[8] Lee 2018: *Verifiable Claims Use Cases.*
[9] Grech 2017: *Blockchain in Education*, S. 27.
[10] ebd.
[11] ebd.
[12] ebd.

Die vorletzte Komponente ist das Zertifikat selbst. Es hält die Identität des Ausstellers, des Empfängers, die Behauptung und, wenn nötig, die Beweise fest. Beispiele für Zertifikate sind Zeugnisse von Schulen und Hochschulen.

Auf dem Zertifikat findet sich auch die letzte Komponente wieder, die Signatur. Dabei handelt es sich um ein einzigartiges Symbol, einen Stempel, ein Bild oder einen Code, der nur vom Aussteller vergeben werden kann und so die Identität des Zertifikats bestätigt.[13]

Eine weitere wichtige Rolle übernehmen Dritte. Dabei handelt es sich um jegliche Personen, die mit dem Zertifikat zu tun haben und keine der anderen Rollen übernehmen. Dies kann beispielsweise eine Firma sein, die daran interessiert ist, die Authentizität eines Zertifikats zu überprüfen.[14]

Dritte sind nicht direkt Teil eines Zertifikats. Sie sind aber insofern wichtig, als dass sie der Hauptgrund sind, warum Zertifikate überhaupt ausgestellt werden. Zertifikate werden genutzt, um Dritten zu demonstrieren, dass die aufgezeichneten Behauptungen über den Empfänger wahr sind. Somit ist die Präsenz und Perspektive von Dritten ein essenzieller Teil von Zertifikaten.

2.1 Eigenschaften von aktuellen, analogen Zertifikaten

Unter aktuellen, analogen Zertifikaten sind vor allem Zeugnisse, die heutzutage auf Papier ausgestellt werden, zu verstehen.

Die Inhaber solcher Zeugnisse können diese zu jeder Zeit überall vorlegen. Die Aufbewahrung und Lesbarkeit der Zeugnisse ist über einen längeren Zeitraum problemlos möglich. Empfänger brauchen keine besonderen Geräte und nur grundlegendes Wissen über das Lagern von Papier. Diese Eigenschaften sind Teil der Gründe, warum analoge Zertifikate bis heute etabliert sind. Beispielsweise nutzen nur wenige Hochschulen bisher digitale Zeugnisse.

2.2 Aktuelle Probleme von analogen Zertifikaten

Bewerbungsverfahren laufen inzwischen weitestgehend digital ab. Analoge Zertifikate sind dabei unmittelbar nur mit Problemen nutzbar. Im Kontrast beispielsweise zum Versenden einer Datei per E-Mail, die auch online überprüft werden kann, ist der Prozess, jemandem ein analoges Zertifikat auf digitalem Weg zukommen zu lassen, umständlicher. Der Überprüfungsprozess ist für Dritte, Aussteller und Empfänger ineffizient und unsicher. Am Beispiel eines Studenten, der sich bei einer Firma bewirbt, die sein Hochschulzeugnis überprüfen möchte, lassen sich mehrere Schwachpunkte erkennen:

Zunächst muss das analoge Zertifikat vom Empfänger gescannt werden, um dieses auf digitalem Weg der Firma zukommen zu lassen. Das Versenden findet per E-Mail oder über eine Webseite, auf der Dateien hochgeladen werden können, statt. Beim Einscannen entsteht bereits die Frage, ob das Zertifikat und die Informationen darauf legitim sind. Eine Datei kann mithilfe von Bildbearbeitungsprogrammen wie Photoshop an dieser Stelle manipuliert werden.

[13] Grech 2017: *Blockchain in Education*, S. 28.
[14] Lee 2018: *Verifiable Claims Use Cases*.

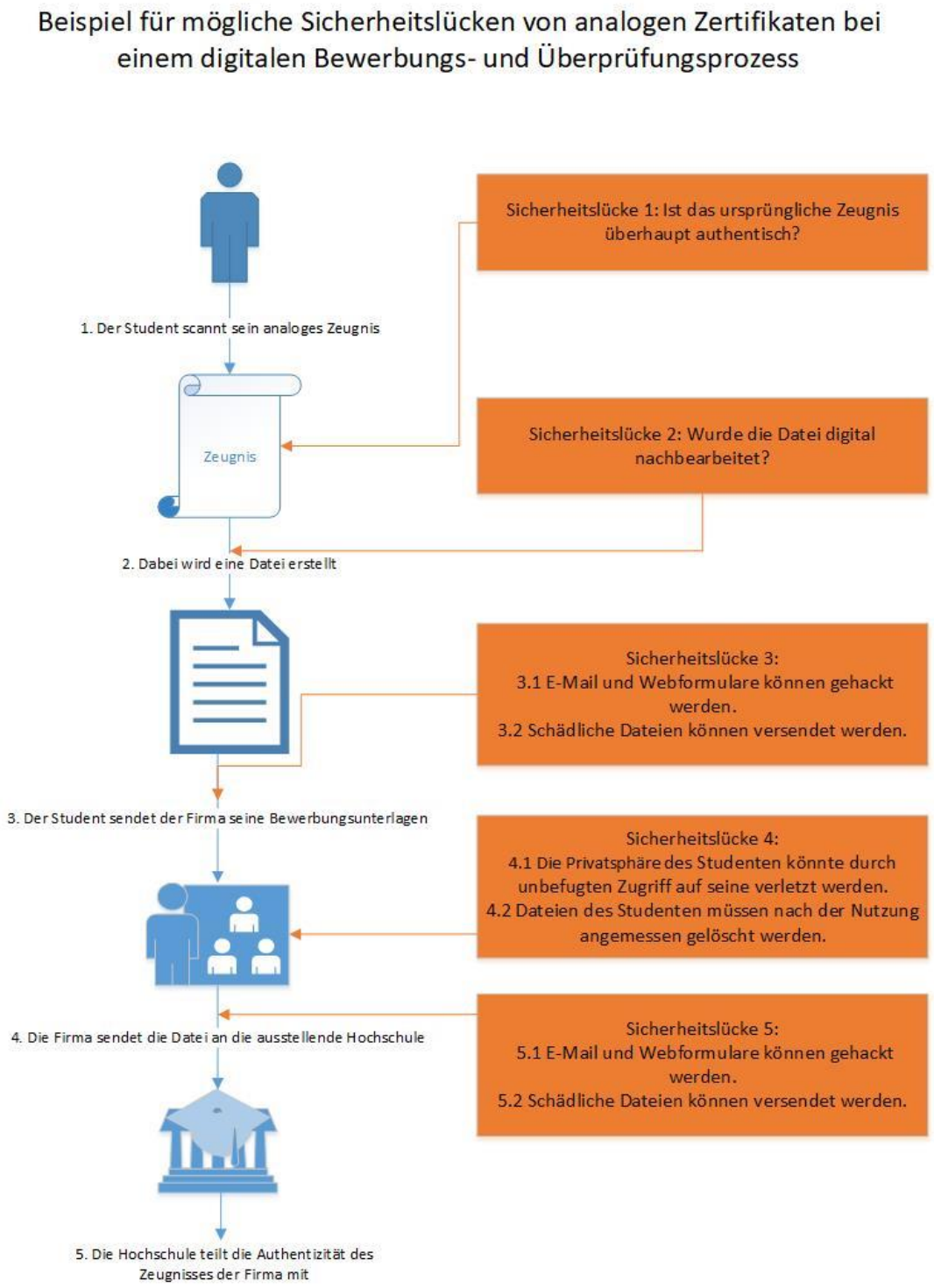


Abbildung 1: Beispiel für mögliche Sicherheitslücken von analogen Zertifikaten bei einem digitalen Bewerbungs- und Überprüfungsprozess

Beim Versenden werden neue Schnittstellen in die Interaktion zwischen Empfänger und Dritten eingeführt, die, wie Hacking-Skandale gezeigt haben, garantiert unsicher sind. Dritte erhalten Dateien, die möglicherweise schädlich sein können. Die erhaltenen Dateien müssen händisch von Personal beurteilt werden, falls keine digitale Form im Bewerbungsprozess vorhanden ist.[15] Dritte müssen diese Dateien zwischenspeichern. Zu diesem Zeitpunkt müssen die Dateien entsprechend gesichert werden. Sicherheitsprobleme können sowohl innerhalb des Unternehmens – in Hinsicht darauf, dass die Privatsphäre des Senders geschädigt werden könnte – als auch außerhalb des Unternehmens entstehen. Selbst große Unternehmen wie Facebook oder Sony sowie auch der private E-Mail-Server der Familie Clinton in den USA zeigen, dass Datenleaks und unbefugte Zugriffe jegliche Personen und Organisationen treffen können und beim Versenden von Daten berücksichtigt werden müssen.

Dritte senden die zu überprüfenden Dateien an den Aussteller, in diesem Beispiel eine Hochschule. Diese Dritten müssen die Dateien wiederum zwischenspeichern und nach der Bearbeitung wieder löschen. Dieser Prozess leidet unter den gleichen Problemen wie derjenige bei der oben beschriebenen Firma. Dazu kommt das Personal, das sich um solche Anfragen kümmert und das Zertifikat überprüfen muss. Dieser Prozess beansprucht Zeit, in de die anderen Beteiligten lediglich warten können.

Falls die Firma in diesem Beispiel sich nicht selbst um diese Aufgabe kümmern will, kann sie auch eine weitere, dritte Partei hinzuziehen, die darauf spezialisiert ist, Zertifikate etc. auf ihre Authentizität hin zu überprüfen. Dies ist allerdings mit weiteren Kosten verbunden und führt eine weitere Schnittstelle in den Überprüfungsprozess ein.

Zu den Problemen des Überprüfungsprozesses kommen weitere Schwachstellen, die analoge Zertifikate aufweisen. Beispielsweise der Verlust sowohl des physischen Originals, das der Empfänger hält, als auch der Verlust des Ausstellers. Dies betrifft aktuell teilweise Flüchtlinge aus dem syrischen Bürgerkrieg.[16] Wenn diese beiden nicht mehr vorhanden sind, ist es für Empfänger nicht mehr unmittelbar möglich, zu beweisen, dass die Behauptungen, die auf dem Zertifikat festgehalten wurden, legitim sind. Ebenso gibt es keine Möglichkeit, diese wiederherzustellen, da der Aussteller und jegliche weitere Dokumentation nicht mehr existieren. Diese Abhängigkeit vom Aussteller kann auch politische Folgen für Empfänger haben. Wenn die fortbestehende Gültigkeit eines Zertifikats daran gebunden ist, dass der Aussteller dieses weiterhin als gültig ansieht, können je nach Land und politischer Lage diese Beziehungen gegen den Empfänger ausgenutzt werden.

Weitere Probleme von analogen Zertifikaten sind beispielsweise, dass das Erstellen von fälschungssicheren analogen Zertifikaten mit verschiedenen Kosten verbunden ist. Je größer die Sicherheit, die in ein Zertifikat eingebaut ist, desto höher sind die damit verbundenen Kosten. Daneben stehen die Transportkosten für das Zertifikat an sich. Diese werden meistens vom Personal des Ausstellers per Post den Empfängern zugesendet. Weitere Kosten betreffen unter Umständen die Arbeit von Personal, das auf Anfragen von Dritten eingehen muss. Dazu kommt die geringe Umweltfreundlichkeit analoger Zeugnisse, da diese auf

[15] Im Kontrast dazu steht beispielsweise eine Jobbörse wie Monster.de. Auf dieser Webseite können Empfänger ihre persöhnlichen Daten eingeben und Arbeitgeber können beispielsweise alle Bewerber auf eine Stelle unter bestimmten Notendurchschnitten automatisch filtern.

[16] Botschaft der Bundesrepublick Deutschland Beirut 2017: *Merkblatt zur Legalisation syrischer Urkunden,* S.2.

Papier erstellt werden. Deutschland ist im internationalen Vergleich weiterhin das Land, das am meisten Papier, Pappe und Karton verwendet.[17]

Die Menge an Arbeit und Kosten, um ein Zertifikat zu fälschen, unterscheidet sich deutlich je nach der Region, in der es erworben wurde, was zu großen regionalen Unterschieden in der Sicherheit von analogen Zertifikaten führt. Während es in Indien möglich ist, einen gefälschten Hochschulabschluss für mehrere hundert Euro zu erwerben,[18][19] vertrauen deutsche Unternehmen sehr auf die Authentizität von analogen Zertifikaten und Scans von diesen (Siehe Anhang 1). Dies führt je nach der Region oder der Herkunft des Ausstellers zu einem unterschiedlichen Grad an Vertrauen in die ausgestellten Zertifikate.

Ein weiterer Bereich, in dem analoge Zertifikate anachronistisch erscheinen, sind Online-Studiengänge und Fernstudium. Heutzutage ist es möglich, Bildung zum größten Teil auf digitalem Weg zu erwerben. Im Kontrast zum Rest dieses Prozesses ist der analoge Hochschulabschluss ein analoges Überbleibsel.

Aus den bisherigen Problemen lässt sich erkennen, dass das analoge Format von Zertifikaten nicht mehr ausreichend ist. Die Nutzung von analogen Zertifikaten in ihrer jetzigen Form führt bei digitalen Prozessen zu Kosten und Sicherheitsproblemen. Zertifikate müssen für digitale Prozesse geupdatet werden, oder es müssen digitale Alternativen entwickelt werden.

[17] Verband Deutscher Papierfabriken 2014: *Pro-Kopf-Verbrauch von Papier, Karton und Pappe im internationalen Vergleich im Jahr 2012 (in Kilogramm je Einwohner).*
[18] Gladstone 2015: *Fake University Degrees Rampant in India.*
[19] Yadav 2018: *Gang of forgers sold 50,000 school and univ degrees, set up fake websites.*

3 Aussteller von Zertifikaten

Das Zeugnis einer Grundschule, ein Hochschulabschluss und eine Badge von Codecademy für das Bearbeiten des HTML-Kurses[20] unterscheiden sich darin, was sie erreichen, bezeugen und in welchem Kontext sie nach dem Erhalt genutzt werden.

Die Bildungsanbieter in diesem Beispiel – eine öffentliche Grundschule, eine öffentliche Hochschule und eine Firma wie Codecademy – teilen Faktoren, die ihren Umgang mit Zeugnissen beeinflussen. Es bestehen aber mehr Unterschiede als Gemeinsamkeiten zwischen diesen Bildungsanbietern. Sie interessieren sich für verschiedene Nutzergruppen und vermitteln unterschiedliche Inhalte. Je nach den Zielen des Bildungsanbieters und den Rahmenbedingungen des Bildungsangebots werden verschiedene Formen zur Vermittlung von Bildung genutzt. Zwar wird bei allen Bildung vermittelt, doch sind der Unterricht in einer Grundschulklasse, die Vorlesung an einer Hochschule und das eigenständige Arbeiten an einem Online-Kurs Ausschnitte aus der Vielzahl an unterschiedlichen Methoden von Bildungsanbietern. Ähnlich sieht es bei der Zertifikation der verschiedenen Bildungsanbieter aus. Deswegen muss zwischen den verschiedenen Ausstellern von Zertifikaten im Bildungsbereich unterschieden werden. Insofern wäre eine umfassende Analyse von Bildungsanbietern sowie der Art und Weise, wie ausgestellte Zertifikate nach dem Erwerb genutzt werden, nötig, um stichhaltige Schlüsse ziehen zu können.

3.1 Öffentliche Bildungsanbieter

Es gibt allerdings eine Gruppe von Bildungsanbietern, die sich auch ohne eine umfassende Analyse aller Bildungsanbieter klar von den anderen Bildungsanbietern abgrenzen lässt. Alle Bildungsanbieter die, ob gesetzlich geregelt oder selbstbestimmt, den öffentlichen Bildungsauftrag verfolgen, haben eine klar definierte Aufgabe. Bei dieser Aufgabe handelt es sich um das Anbieten von Bildung für die Öffentlichkeit. Öffentlich Bildung anzubieten rechtfertigt das Fortbestehen dieser Bildungsanbieter.

In dieser Hinsicht lässt sich eine klare Grenze zwischen dieser Gruppe und anderen Bildungsanbietern ziehen. Andere Bildungsanbieter können beispielsweise kommerzielle Interessen oder andere Ziele verfolgen. Unter Berücksichtigung dieser Aufgabe sowie der Eigenschaften und aktuellen Probleme von analogen Zertifikaten im Bildungsbereich lässt sich ein Kriterienkatalog mit einer klaren Gewichtung zwischen aktuellen und digitalen Alternativen erstellen.

3.2 Weitere Bildungsanbieter

Im Kontrast zu öffentlichen Bildungsanbietern kann die heterogene Gruppe weiterer Bildungsanbieter von ebenso heterogenen Interessen geleitet werden. Um für diese Gruppe klare Handlungsempfehlungen auszusprechen, müssten die relevanten Interessen dieser Bildungsanbieter untersucht werden. Das würde den Rahmen der vorliegenden Arbeit sprengen. Deswegen richtet sie sich nicht direkt an diese Gruppe.

Trotzdem können alle Bildungsanbieter die Ergebnisse dieser Arbeit berücksichtigen und die Handlungsempfehlungen und Schlüsse nutzen. Denn solange die Ziele eines Bildungsanbieters auch nur

[20] Codecademy: *About Points, Badges, and Streaks.*

teilweise mit den Zielen der öffentlichen Bildungsanbieter übereinstimmen, sind die Handlungsempfehlungen und Schlüsse auch für sie relevant.

4 Typologie digitaler Alternativen

Es gibt eine Typologie, die darauf abzielt, mithilfe von Blockchain einen Überblick aktueller Lösungen im Bereich digitaler Zertifikate zu liefern. Diese Typologie kommt aus einem öffentlichen Blogpost des CEO von Learning Machine, einer Firma, die selbst Software für auf Blockchain basierende Zertifikate entwickelt.[21] Eine andere und ähnliche Typologie befasst sich mit der Perspektive von Archiven im Hinblick auf auf Blockchain basierenden Umsetzungen zur Dokumentation.[22] Im Kontrast zur erstgenannten Typologie lassen sich die in dieser Typologie beschriebenen Types allerdings nicht ohne Weiteres auf die im Bildungsbereich genutzten Umsetzungen übertragen.

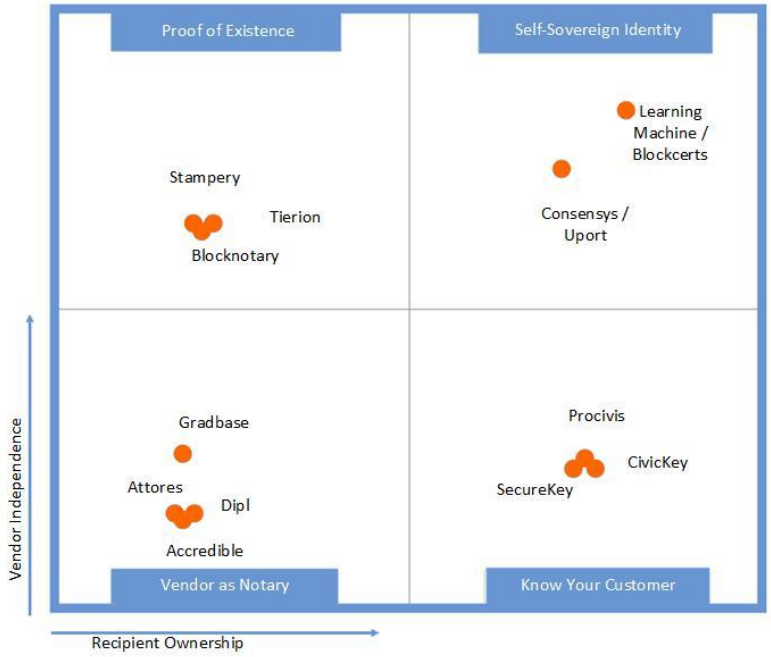


Abbildung 2: Typologische Übersicht[23]

In der genutzten Typologie gibt es vier verschiedene Types. Diese werden nach zwei Achsen angeordnet: der Unabhängigkeit gegenüber dem Aussteller auf der y-Achse und dem Eigentum des Empfängers auf der x-Achse. Mit „Recipient ownership“ (Unabhängigkeit gegenüber dem Aussteller) ist gemeint, dass Empfänger die privaten Schlüssel besitzen, um zu demonstrieren, dass sie ihre digitalen Zertifikate besitzen. Mit „ Vendor Independence“ (Eigentum des Empfängers) ist gemeint, wie viel Einfluss und Kontrolle der Empfänger über das erhaltene Zertifikat hat. Durch diese beiden Kategorien ergeben sich vier Quadranten, in denen unterschiedliche Zustände und Abhängigkeiten für alle bei der Erstellung und Nutzung von Zertifikation beteiligten Parteien und Komponenten herrschen. Mit dieser Art von Kategorisierung können die verschiedenen Umsetzungen von Zertifikaten eingeordnet werden, selbst wenn Blockchain nicht Teil der Umsetzung ist. Berücksichtigt werden muss allerdings, dass die verschiedenen Types Eigenschaften und Dienstleistungen teilen können und gleichzeitig zu verschiedenen Types gehören. Es handelt sich dabei also um keine trennscharfen Kategorien.

[21] Jagers 2017: *Digital Identity and the Blockchain.*
[22] Lemieux 2017: *A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation,* S.4-8.
[23] Nachbildung von https://cdn-images-1.medium.com/max/1043/1*Rg3XwxlglULjsmRy4FQXtg.png aus: Jagers 2017: *Digital Identity and the Blockchain.*

4.1 Proof of Existence (PoE)

Proof-of-Existence-Types sind auf dem Feld der Typologie im oberen linken Quadranten zu finden. Sie weisen eine hohe Unabhängigkeit vom Aussteller, aber einen niedrigen Grad an Eigentum des Empfängers auf. Bei Proof-of-Existence-Modellen wird Blockchain genutzt, um die fortbestehende Integrität von Daten zu demonstrieren.

Auf technischer Ebene wird bei Proof-of-Existence-Modellen mithilfe von Hashes (auch als „digitaler Fingerabdruck" bezeichnet) die Integrität von Daten gesichert. Hashes sind eine einzigartige Sequenz von Zahlen und Buchstaben, die mithilfe von kryptografischer Verschlüsselung, beispielsweise dem SHA-256-Algorithmus, erstellt werden. Der String „abc123" resultiert beispielsweise in dem Hash „6CA13D52CA70C883E0F0BB101E425A89E8624DE51DB2D2392593AF6A84118090".[24]

Aus einem Hash kann ein Dokument nicht rekonstruiert werden. Aber ein Dokument kann beliebig oft gehasht werden. Solange das Dokument nicht auf irgendeine Weise verändert wurde, wird weiterhin derselbe Hash generiert. Bei einer Veränderung der Datei findet ebenfalls eine Veränderung des generierten Hashes statt. Diese generierten Hashes werden dann auf einer Blockchain festgehalten.

Wenn die zu überprüfende Datei denselben Hash hat, der auf der Blockchain festgehalten ist, ist die Authentizität der Datei gewährleistet. So wird in diesem Modell Blockchain als Werkzeug zur permanenten und öffentlichen Speicherung der Hashes genutzt. Deswegen ist es unbedingt erforderlich, zu verstehen, wie die Sicherheit von Blockchain funktioniert, um den Type korrekt zu identifizieren.

Am Beispiel der Bitcoin (BTC) Blockchain, die für solche Umsetzungen oft genutzt wird, lässt sich dies erklären. Bei Bitcoin werden Transaktionen zwischen Adressen (die Nutzer auf der Blockchain) aufgezeichnet. Diese werden in Blocks zusammengefasst und in der nachfolgend geschilderten Reihenfolge gespeichert. Es handelt sich bei Blockchain also um eine Art von verteiltem Kontoführungsjournal.

Bei dem Netzwerk, auf dem diese Transaktionen stattfinden, handelt es sich um ein Peer-to-Peer-Netzwerk, in dem keine zentrale Instanz vorhanden ist. Das Netzwerk selbst wird also von den Teilnehmern des Netzwerks betrieben. Teilnehmen an diesem Netzwerk kann jeder, der eine eigene Kopie des bisherigen Journals (der bisherigen Blockchain) von anderen Teilnehmern des Netzwerks herunterlädt. Einzelne solche Teilnehmer, mit eigenen Kopien der bisherigen Blockchain, werden auch als Node bezeichnet. Besitzer dieser Nodes werden als Miner bezeichnet.[25] Auf diese Weise weiß jeder Teilnehmer am Netzwerk auch über alle anderen Transaktionen des Netzwerks Bescheid.

Jedes Mal, wenn ein Teilnehmer eine Transaktion an das Journal einreicht, überprüfen die Nodes, ob die Transaktion auch valide ist, das heißt, ob der Teilnehmer, der ein Bitcoin ausgeben will, auch tatsächlich ein Bitcoin besitzt. Ein Teil der Nodes konkurrieren darum, valide Transaktionen in „Blocks" zusammenzufassen und der bisherigen Kette von Blöcken hinzuzufügen.[26]

[24] Mithilfe von „Passwordgenerator.net: *SHA256 Hash Generator"* erstellt.
[25] Orcutt 2018: *How secure is blockchain really?.*
[26] ebd.

Die Entscheidung, wie und welcher Block als Nächstes gespeichert wird, wird mit einem mathematischen Problem bestimmt. Für jeden neuen Block wird automatisch ein neues Problem vom Bitcoin Protokoll generiert. Beim Lösen dieses mathematischen Problems wird am Ende ein Hash generiert. Bei diesem Hash handelt es sich um den Hash des Blocks. Jeder nachfolgende Block hat den Hash des Blocks davor in sich. Daher kommt auch das „chain" in „Blockchain".

Die Node, die das Problem als Erstes löst, fügt der bisherigen Blockchain den nächsten Block hinzu. Für das erfolgreiche Hinzufügen eines neuen Blocks gibt es eine Belohnung vom Protokoll in Form von Bitcoin Token. Diese Belohnung entsteht einerseits aus den Kosten für Transaktionen und andererseits aus der Verteilung der absoluten Anzahl von Bitcoins.

Wenn andere Nodes zu demselben Ergebnis kommen wie die erste Node, wird der Block bestätigt und gilt als etabliert. Kommen die Nodes zu einem anderen Ergebnis, wird von ihrer Mehrheit ein neuer Block als korrekter, nächster Block identifiziert.

Das Lösen des mathematischen Problems kostet eine große Menge an Rechenarbeit und damit Elektrizität. Seit dem 9. Juni 2018 beträgt der Stromverbrauch von Bitcoin konstant etwas über 71 TWh pro Jahr. Damit steht der Stromverbrauch von Bitcoin momentan zwischen dem jährlichen Stromverbrauch der Tschechischen Republik, mit 67,3 TWh pro Jahr, und Chile, mit 71,7 TWh pro Jahr.[27]

In der Bitcoin Blockchain werden Blöcke chronologisch aneinandergereiht. Wenn jemand beispielsweise den letzten Block, der zur Blockchain hinzugefügt wurde, manipulieren möchte, wird dafür dieselbe Menge an Energie benötigt, wie sie für die Bestätigung des Blocks aufgebracht wurde. Wenn jemand allerdings Blöcke manipulieren möchte, die vor einer längeren Zeit in die Blockchain geschrieben wurden, beispieslweise der fünfzigste Block vor dem letzten, der hinzugefügt wurde, muss die Energie für alle bisher bestätigten Blöcke aufgebracht werden. Die Menge an Energie, um diesen Block zu verändern, beträgt also die Summe der aufgebrachten Energie für die letzten fünfzig Blöcke. Je früher also die Transaktion in der Blockchain stattgefunden hat, desto größer ist die Menge an Energie, die aufgebracht werden muss, um an den vorherigen Blöcken etwas zu ändern.

Bei einer Transaktion auf der Bitcoin Blockchain können zusätzliche Daten (in eingeschränktem Rahmen) auf der Blockchain gespeichert werden. Wenn beispielsweise eine Datei gehasht wurde, kann dieser Hash bei einer Transaktion hier eingefügt werden, sodass er auf der Bitcoin Blockchain festgehalten wird. Da nur der Hash auf der Blockchain zu finden ist, werden keine persönlichen Informationen auf dieser gespeichert. Solange der Hash der Datei und der Hash in der Blockchain gleich sind, ist die Datei unverändert. Proof of Existence als Type demonstriert auf diese Weise das mögliche unveränderte Fortbestehen einer Datei.

Damit Proof of Existence zur Sicherung genutzt werden kann, muss im Voraus vom Aussteller ein digitales Zeugnis erstellt werden. Dabei kann es sich auch um eine digitale Repräsentation eines analogen Zeugnisses handeln, beispielsweise um einen Scan des Originals. Die Sicherheit ist nicht im Zertifikat selbst zu finden. Die Sicherheit befindet sich in der Komponente, die das Unverändertsein einer Datei belegen kann, die Blockchain.

[27] Digiconomist: *Bitcoin Energy Consumption Index.*

Der Grund, warum Blockchain hier so kritisch für die Definition des Types ist, liegt darin, dass es wenige Alternativen mit gleichen Stärken gibt. Bitcoin und ähnliche Blockchains sind eine sichere und öffentliche Methode, Daten auf lange Zeit unveränderbar zu speichern. Technisch gesehen könnte allerdings jede Methode, die versucht mithilfe von Hashes oder auf ähnliche Weise die Authentizität von Daten auf lange Zeit zu sichern, zu diesem Type gehören – auch ohne Blockchain.

Ein Beispiel für eine Firma, die eine Proof-of-Existence-Umsetzung anbietet, ist Stampery. Stamperys Dienstleistungsangebot besteht in der digitalen Notarisierung von Dateien, Dokumenten und E-Mails mithilfe der Blockchains von Bitcoin und Ethereum (ETH). Stampery nutzt die vorher beschriebenen Prozesse, wobei noch ein weiterer Schritt hinzukommt. Bevor ein Hash auf die Blockchain geschrieben wird, wird er gemeinsam mit den Hashes von weiteren Dateien in einem Merkle-Baum kombiniert.

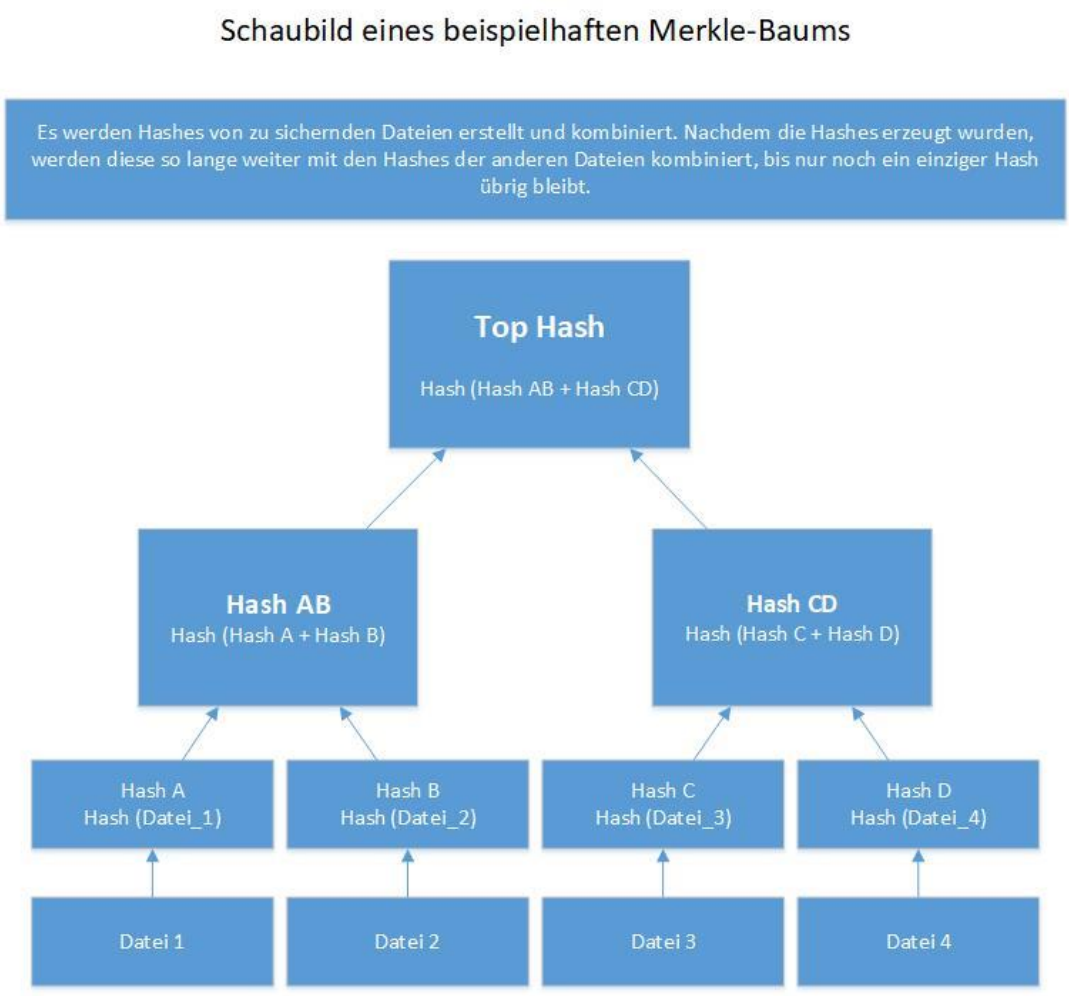


Abbildung 3: Beispiel eines Merkle-Baums[28]

[28] Nachbildung von https://de.wikipedia.org/wiki/Hash-Baum#/media/File:Hash_Tree.svg.

Der Top Hash, auch Merkle-Wurzel genannt, des Merkle-Baums wird daraufhin in die Blockchain eingetragen. Durch Nutzung von Merkle-Bäumen kann eine wesentlich größere Anzahl von Hashes gebündelt und auf die Blockchain eingetragen werden. Dieser Schritt wird von den meisten Anbietern dieses Sektors in den Zeitstempel-Prozess eingebaut, da es den Anbietern und Nutzern viele Vorteile schaffen kann und Engpässen entgegenwirkt.

Der größte Klient der Firma ist das Land Estland. Gemeinsam bieten die beiden die „e-Resident digi-ID card" an. Dabei handelt es sich um ein Identifikationsdokument mit dessen Hilfe ortsunabhängige Unternehmen online zu E-Residenten werden können. E-Residenz soll eine sichere und praktische Methode sein, um digitale Dienstleistungen online glaubwürdig auszuführen.[29] Es handelt sich dabei nicht um ein Dokument, das eine Bürgerschaft oder Ähnliches verleihen soll. Vielmehr sollen Unternehmen darin unterstützt werden, dass sie von einem europäischen Staat und mithilfe von Blockchain gesicherte und vertrauenswürdige Transaktionen und Dokumentationen anbieten können. Mithilfe dieser E-Residenz kann Stampery für jegliche Dateien und Dokumente genutzt werden. Dabei besteht eine doppelte Garantie von Vertrauen, sowohl von der Blockchain her als auch von dem Aussteller der E-Residenz, dem estnischen Staat her.

Ein weiterer Konkurrent auf dem Markt von Proof-of-Existence-Umsetzungen ist Tierion. Auch Tierion nutzt Merkle-Bäume in seinem „Chainpoint"-Protokoll[30]. Je größer die Umsetzung skalieren soll, desto höher sind die Chancen, dass die Proof-of-Existence-Umsetzung auch eine Methode zum Bündeln von einzelnen Hashes besitzt.

Während diese beiden Konkurrenten auf Unternehmen und Organisationen abzielen, gibt es auch Teilnehmer am Markt, die für einzelne Nutzer ihr Angebot bereitstellen. Beispielsweise gibt Originstamp jedem Nutzer die Möglichkeit, Dateien kostenlos zu sichern. Allerdings benutzt selbst dieser Anbieter, der eine niedrigere Anzahl von Nutzern verzeichnet, das Bündeln von Hashes. Einmal am Tag werden von Originstamp die Hashes gebündelt und auf die Bitcoin Blockchain geschrieben.[31]

[29] Estonian Police and Border Guard Board: *Application for e-Residency.*
[30] Riley 2018: . *Creating an immutable audit trail on the blockchain with Xero & Tierion.*
[31] Originstamp: *Free trusted timestamping.*

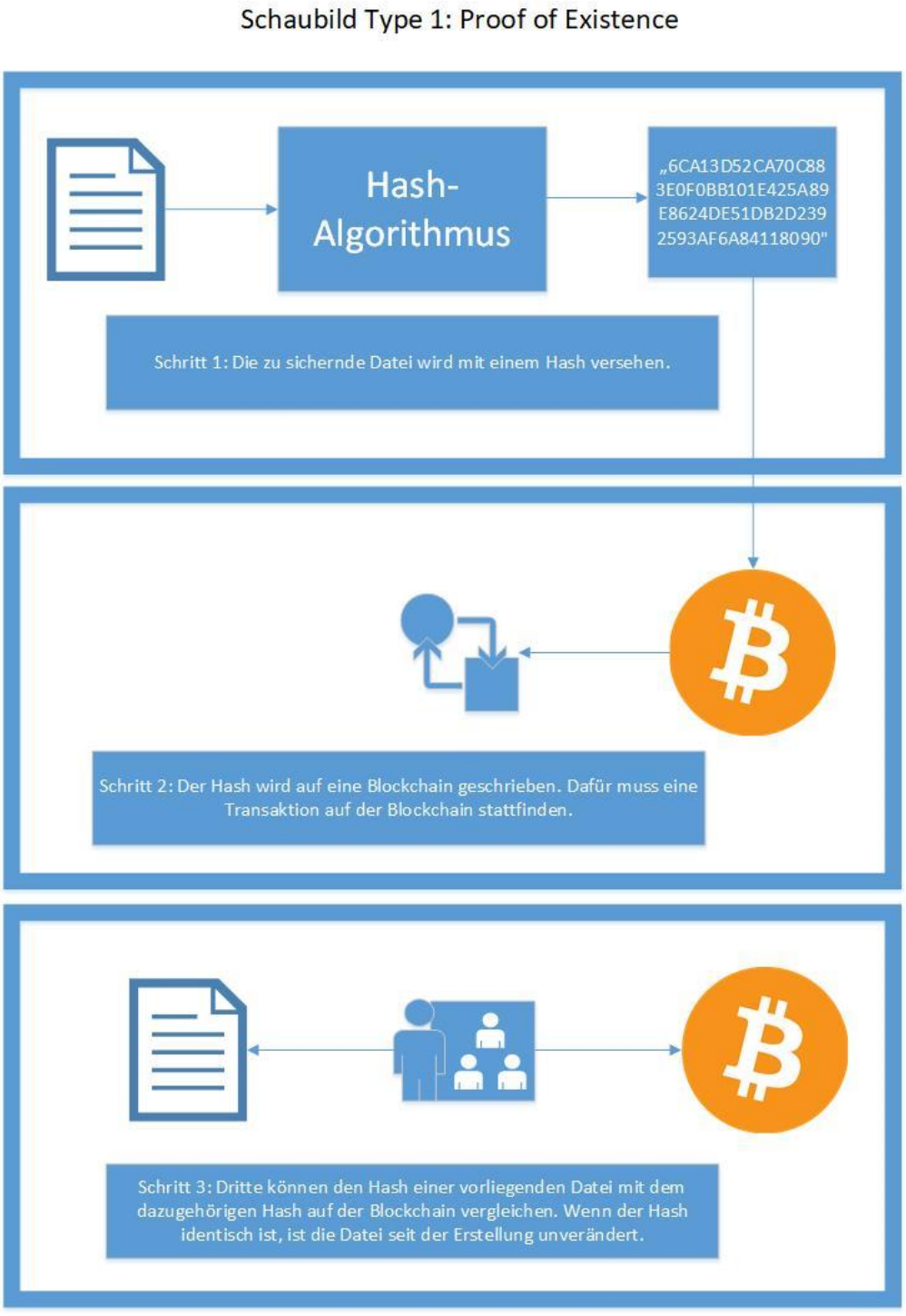


Abbildung 4: Schaubild Type 1: Proof of Existence

4.2 Vendor as Notary (VaN)

Das Vendor-as-Notary-Modell befindet sich im unteren linken Quadranten in Abbildung 2. Hier liegt eine niedrige „Unabhängigkeit gegenüber dem Aussteller“ sowie auch ein niedriges „Eigentum des Empfängers“ vor. Im Vendor-as-Notary-Type ist der Aussteller des Zertifikats oder eine dritte Partei auch für den Zugriff und die Sicherung des Zertifikats zuständig. Wie genau hier die technische Umsetzung letztendlich funktioniert, ist nicht entscheidend und oft nicht absehbar, ohne direkten Zugriff auf Informationen darüber, wie der Anbieter seine Zertifikate erstellt und bereitstellt. Der definierende Faktor ist, dass der Aussteller oder eine dritte Partei (beispielsweise eine Firma, die sich auf diese Aufgabe spezialisiert) die Kontrolle über das Systems ausübt.

Ein Beispiel für einen kommerziellen Anbieter in diesem Bereich ist Accredible. Accredible ist eine kommerzielle Plattform, auf der sowohl digitale Zertifikate als auch Open Badges ausgestellt und verwaltet werden können (siehe Anhang 2).

Zertifikate und Badges können innerhalb des Portals von Nutzern ausgestellt werden. Dies funktioniert über die beiden Design-Editoren. Dort können mithilfe von Templates und der Möglichkeit des Hochladens weiterer Bilder die Zertifikate und Badges von Nutzern designt werden. Um ein Zertifikat an eine Person auszustellen, werden der Name des Empfängers und seine E-Mail-Adresse benötigt.

Es können von Nutzern auch spezifische Gruppen erstellt werden. Das Ziel dieser Funktion ist es, Speichern, Management und Ausstellen von verschiedenen Zertifikaten und Badges zusammenzubringen.[32] Beim Erhalten eines Zertifikats wird Empfängern ein Link zu einer von Accredible betriebenen Website zugeschickt. Auf dieser Seite ist dann das ausgestellte Zertifikat zu finden.

Wenn Nutzer mit einer E-Mail bestätigen, dass sie tatsächlich die Empfänger des Zertifikats sind, bekommen sie nach einem Pop-up zur Kontoerstellung oder temporären Nutzung von Accredible Zugriff auf die Privatsphäre-Optionen ihres Zertifikats. Darüber hinaus können an dieser Stelle von Empfängern Beweise und Personen, die auch Konten bei Accredible haben, als Referenzen für ein Zertifikat hinzugefügt werden.

Eine weitere Funktion von Accredible ist das Analytics-Fenster. Aufgezeichnete Daten können je nach Gruppen und Zeiträumen untersucht werden. Die aufgezeichneten Daten sind in vier Bereiche aufgeteilt:

- die Anzahl von ausgestellten Zertifikaten und Badges,
- „Recipient Engagement“ , in dem Daten zur Nutzung der Funktionen von Empfängern der Zertifikate aufgezeichnet werden,
- dem Marketingwert, in dem das Formular einen Wert in US-Dollar generiert, der den dazugewonnenen Wert durch Referenz des Zertifikats aufzeigen soll,
- die Teilstatistik, in der aufgezeichnet wird, wie oft Zertifikate auf Twitter, Facebook, Google+ und E-Mail geteilt wurden.

[32] Accredible: *What is a group?.*

Darüber hinaus gibt es die Möglichkeit, diese Daten zu exportieren und eine Liste jeglicher Ereignisse in Bezug auf die Zertifikate einzusehen. Diese Option steht den Empfängern von Zertifikaten nicht zur Verfügung.

Anders als viele andere Anbieter zeigt Accredible teilweise öffentlich Preise für sein Produkt an.[33]

Blockchain wird in dieser Methode meistens auf die gleiche Weise wie im Proof-of-Existence-Type genutzt. Da hier allerdings ohnehin eine Abhängigkeit vom Aussteller besteht, spielt Blockchain hier eine weniger wichtige Rolle. Das Versehen eines Zertifikats mit einem permanenten Blockchain Timestamp ist eine optionale Funktion. Insofern kann diese Methode auch ohne Blockchain gelöst werden, wie beispielsweise die Universität Göttingen demonstriert. Unabhängig von einer Blockchain liegt die Sicherheit des Zertifikats bei dem Anbieter der Infrastruktur. Insofern kann das System der Universität Göttingen als Beispiel für diesen Type ohne Blockchain genutzt werden. Neben einem analogen Zeugnis wird eine offizielle, digitale Abbildung desselben erstellt (siehe Anhang 3).

Bei erfolgreichem Abschluss des Studiums erhalten Studenten eine E-Mail mit einer deutschen und einer englischen Zeugnis-PDF sowie einer kurzen Beschreibung, wie diese Dateien genutzt werden können. Die Zeugnis-PDFs bestehen aus Scans des analogen Originals und des „Deckblatts zur Aktenablage der Zeugnisdokumente“ sowie einer digitalen Version der Zeugnisse.

Auf dem Original und auf der digitalen Version befinden sich ein Link und ein Passwort. Der Link führt zu einem Überprüfungsportal der Hochschule. Auf diesem Portal kann mithilfe des Passworts die bestätigte, digitale Abbildung des Originals gefunden werden. Auf diese Weise kann die vom Empfänger vorgelegte Version des Zertifikats, egal ob analog oder digital, auf digitalem Weg überprüft werden. Solange die vorgelegte und die von der Hochschule bereitgestellte Version identisch sind, handelt es sich um ein authentisches Zertifikat.[34]

[33] Accredible: *Certificate and Badge Pricing*.
[34] Radenbach 2018: *Elektronische Zeugnisse und Verifikation* . S. 13, 28.

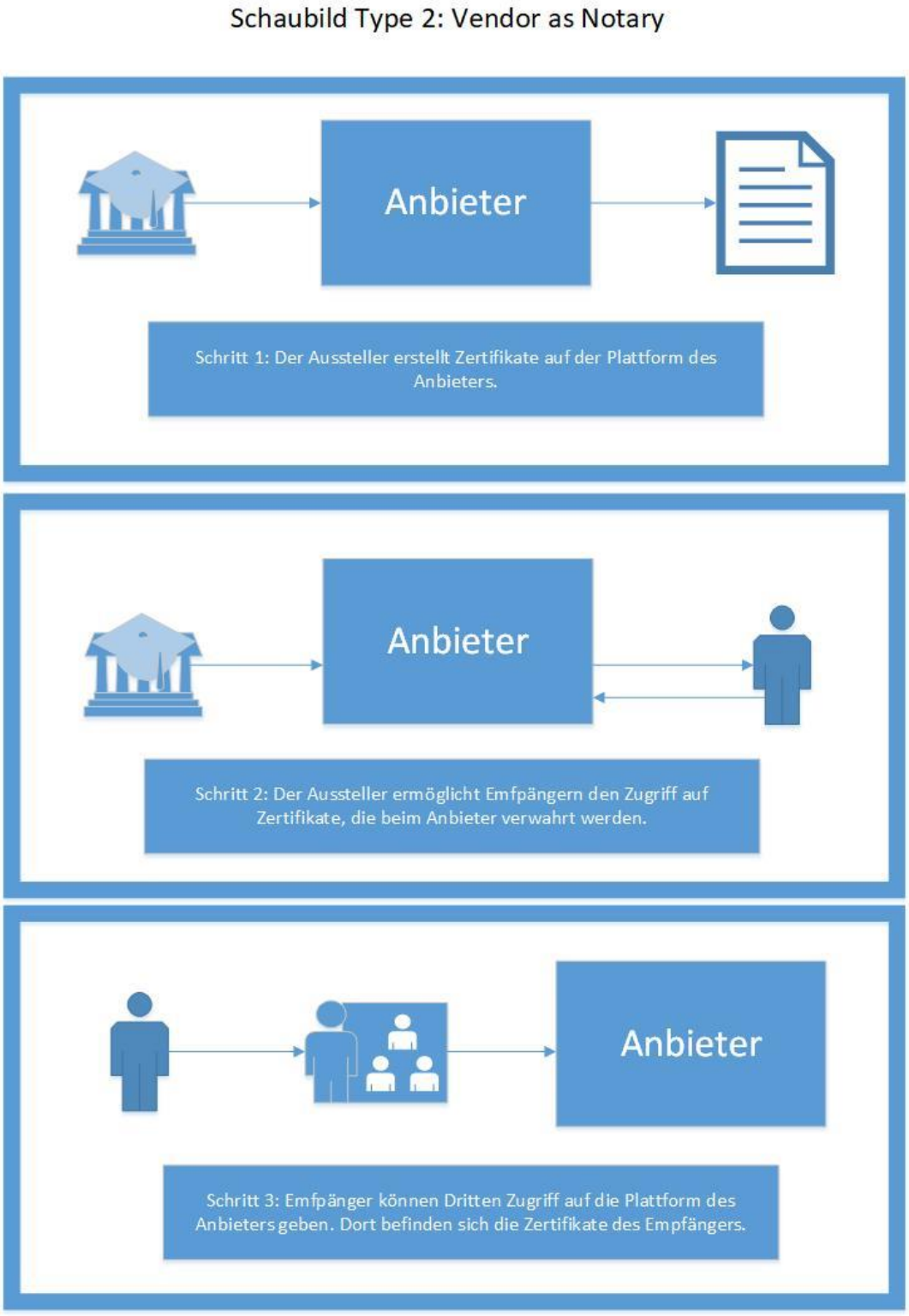


Abbildung 5: Schaubild Type 2: Vendor as Notary

4.3 Know Your Customer (KYC)

Der Know-Your-Customer-Type befindet sich im unteren, rechten Quadranten der Typologie. Es herrscht eine niedrige Unabhängigkeit vom Aussteller und eine hoher Eigentum von Zertifikaten. In diesem Type wird ein System (meistens von Dritten) erstellt, in dem Behauptungen von Zertifikaten als authentisch festgehalten werden können. Alle Teilnehmer des Systems können dann vom Empfänger des Zertifikats – mit dessen Erlaubnis – Zugriff auf die Bestätigung der Authentizität der Behauptungen des Zertifikats erhalten. Eine wichtige Rolle beim Know-Your-Customer-Type spielt also das Überprüfen von Zertifikaten und Behauptungen.[35]

Der Name des Types und die entscheidenden Eigenschaften sind beide an einem bestimmten Prozess der Legitimationsprüfung, die meistens im Finanzwesen genutzt wird, orientiert. Bei dem Prozess handelt es sich um eine detaillierte Prüfung von bestimmten relevanten Informationen über die infrage stehenden Personen. Meistens handelt es sich bei den Überprüfern in solchen Systemen um vertraute Einrichtungen oder Kunden des Besitzers des Systems, beispielsweise Banken oder öffentliche Einrichtungen. An dieser Stelle können auch Hochschulen diese Arbeit übernehmen. Blockchain wird in diesem Type auf die gleiche Weise wie in den vorherigen Types genutzt, nämlich zum öffentlichen Langzeitspeichern von Daten.

Ein Beispiel für so ein System, das Blockchain benutzt, ist Civic. Civic bietet eine selbst entwickelte App an, mit deren Hilfe Anfragen an Informationen zur Identität von Nutzern gemacht werden können. Nutzer tragen in die App die Informationen und Behauptungen ein, die sie überprüfen lassen möchten, und diese Informationen werden auf dem Mobiltelefon mit der App lokal gespeichert. Um die Behauptungen überprüfen zu lassen, müssen Nutzer meistens Beweise an die Überprüfer des Systems senden. Dies ist beispielsweise nicht der Fall, falls es sich um einen Studenten handelt, der von der Hochschule, an der er seinen Hochschulabschluss erworben hat, überprüft werden soll. In diesem Fall besitzt der Überprüfer (die Hochschule) bereits eigene Aufzeichnungen und Beweise über die Behauptungen des Studenten. Die Wahl des Überprüfers fällt auf Dritte, die an der Authentizität von Behauptungen interessiert sind.[36] Im genannten Beispiel könnte der Student sich bei einer Firma bewerben. Wenn die Firma die Behauptungen des Studenten überprüfen möchte, kann sie sich einen Überprüfer für diese Aufgabe aussuchen, falls bisherige Überprüfer ihr nicht ausreichend sind. Wenn der Nutzer einverstanden ist, diesem Überprüfer zu vertrauen, findet die Überprüfung statt.

Wenn die angegebenen Informationen erfolgreich überprüft worden sind, werden sie einzeln gehasht und in einem Merkle-Baum zusammengebracht. Der Top-Hash wird daraufhin mit zufälligen Zahlen versehen und auf die Bitcoin Blockchain geschrieben.[37] Auf diese Weise sollen Nutzer die Möglichkeit bekommen, nur solche Informationen zu teilen, die sie auch wirklich teilen wollen.

Nachdem die Informationen validiert wurden, können Nutzer nun die App benutzen, um bei weiteren Teilnehmern des Systems Behauptungen über ihre Identität bestätigen zu lassen. Wenn eine Anfrage auf Informationen an einen Nutzer gestellt wird, kann dieser auswählen, welche Informationen geteilt werden sollen – und welche nicht. Die Informationen, die der Nutzer an Dritte gibt, werden dann automatisch mit

[35] Civic 2018: *Token Behavior Model*. S. 4.
[36] ebd.
[37] Civic 2017: *Whitepaper*. S. 14.

den von der App auf der Blockchain festgehaltenen Informationen verglichen. Falls es sich um die gleichen Hashes bei beiden Informationen handelt, sind die Informationen identisch.

Zum Betreiben dieses Systems nutzt Civic eine eigene Kryptowährung, die ebenfalls Civic (CVC) heißt. CVC wird in diesem Wirtschaftssystem als Währung genutzt:„To create a decentralized identity management network that exhibits a high level of accuracy by making use of embedded incentives that reward good behavior (accuracy) in die digital identity ecosystem, and discourage bad behavior with penalties.“[38]

[38] Civic 2018: *Token Behavior Model*. S. 5.

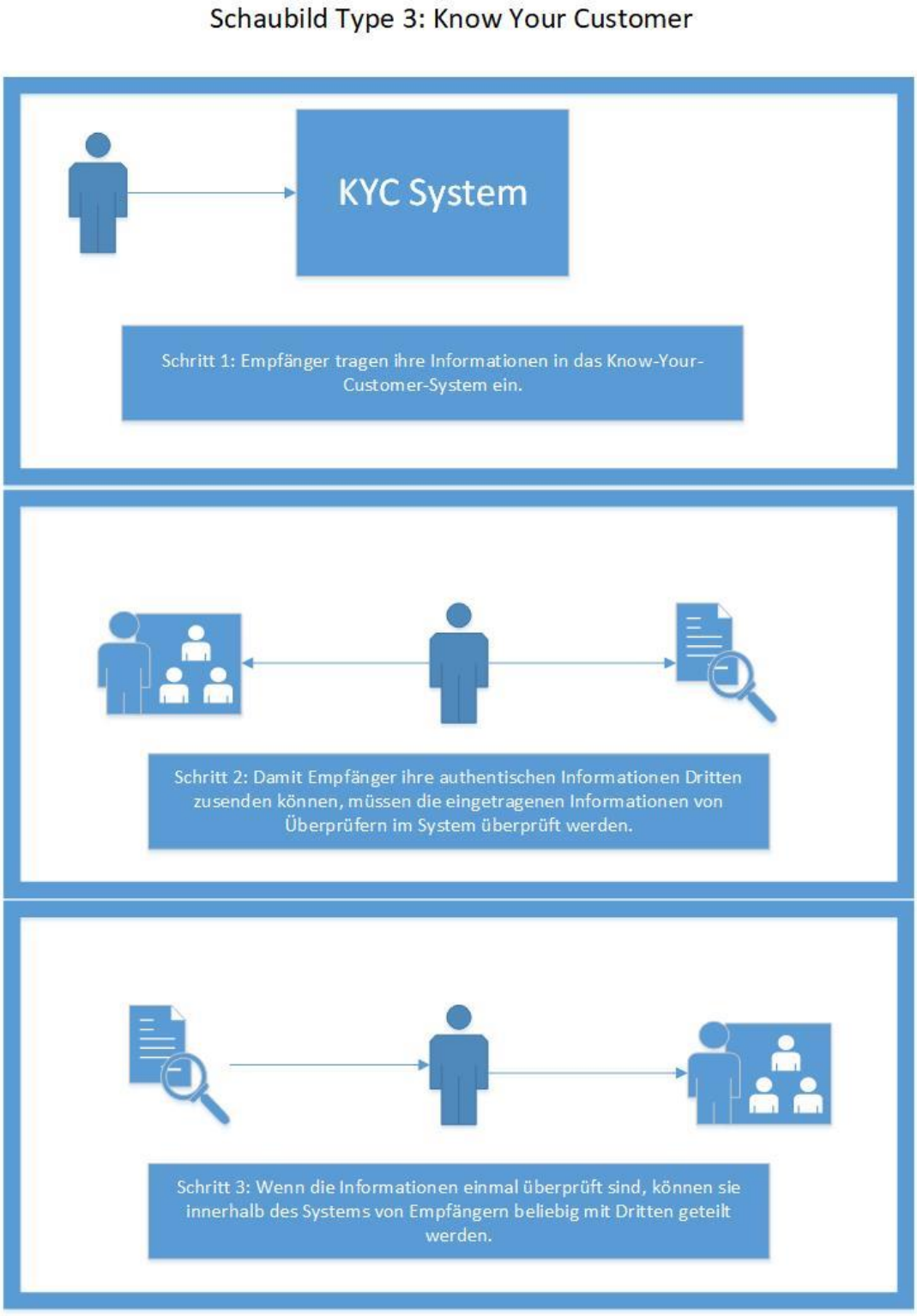


Abbildung 6: Schaubild Type 3: Know Your Customer

4.4 Self-Sovereign Identity (SSI)

Dieser Type von Zertifikaten findet sich im oberen rechten Quadranten. Er zeichnet sich durch eine hohe „Unabhängigkeit gegenüber dem Aussteller“ und ein hohes „Eigentum des Empfängers“ bezüglich der eigenen Zertifikate aus. In dieser Hinsicht unterscheiden sich self-sovereigne Types von den bisherigen Types: Sie zielen darauf ab, eine neue Form von digitaler Zertifikation einzuführen, die unabhängig vom Aussteller oder von Dritten als authentisch anerkannt werden kann.[39]

Der Self-Sovereign-Identity-Type unterscheidet sich fundamental von den bisherigen Types. Am Beispiel von Blockcerts soll er näher charakterisiert werden. Umsetzungen dieses Types zielen darauf ab, die Ziele und Anforderungen, die an Self-Sovereign Identity[40] gerichtet werden, für den Bildungsbereich umzusetzen. Bei Self-Sovereign Identity handelt es sich um bestimmte Prinzipien, die von Dokumenten, die Informationen zur Identität einer Person aussagen, eingehalten werden sollen. Dabei handelt es sich hauptsächlich bei der Implementation von Blockcerts um den Besitz der eigenen Zertifikate, um die volle Kontrolle von Empfängern und um die Gültigkeit unabhängig vom Aussteller.

Das soll durch die Kombination von drei verschiedenen Maßnahmen erreicht werden:

1. Aufzeichnungen sollen im Format von offenen Standards ausgestellt werden.[41]
2. Ausgestellte Aufzeichnungen sollen die öffentlichen Blockchainadressen von Empfängern enthalten.[42]
3. Das Halten von Aufzeichnungen soll in einem Open-Source-Behälter stattfinden, beispielsweise einer App von Blockcerts.[43]

In Kontrast zu den bisherigen Types ist dieser Type technisch schwieriger einzugrenzen. Die bisher entwickelten und öffentlichen Umsetzungen dieses Types unterscheiden sich in ihrer technischen Struktur. Sie zielen aber fundamental auf das gleiche Ziel ab. [44] Deswegen ist dieser Type von der Eingrenzung, welche Umsetzungen zu ihm gehören, anders als die bisher genannten.

Da Blockcerts eigentlich nur ein offener Standard für digitale Zertifikate ist, wird ein Beispiel von einer konkreten Blockcerts-Umsetzung benötigt: Ein solches Beispiel sind die „digital diplomas“ am MIT. Gemeinsam mit der Firma Learning Machine werden dort digitale Zertifikate auf der Basis von Blockcerts Standards ausgestellt.[45]

Das Ausstellen von Zertifikaten mit dem Blockcerts-Standard unterscheidet sich nicht grundlegend von den bisherigen Types. Zunächst muss der Aussteller die öffentliche Adresse auf einer unterstützten Blockchain (momentan Bitcoin und Ethereum) eines Empfängers von diesem erfragen. Daraufhin versieht der Aussteller ein digitales Zeugnis mit seiner Signatur und speichert den Hash dieser Datei in einer Blockchain-

[39] Jagers 2018: *The New Blockcerts Mobile App.*
[40] English 2017: *The Path to Self-Sovereign Identity.*
[41] Jagers 2017: *Digital Identity and the Blockchain.*
[42] ebd.
[43] ebd.
[44] Mehrain 2016: *Blockchain Enabled Self-Sovereign Identity.*
[45] Durant 2017: *Digital Diploma debuts at MIT.*

Transaktion. Die Transaktion geht von der öffentlichen Adresse des Ausstellers an die öffentliche Adresse des Empfängers.[46] Auf diese Weise wird nicht nur die Authentizität der Behauptungen festgehalten, es wird auch unzweifelhaft klar, wer die beteiligten Personen sind.

Das Überprüfen von Zertifikaten kann mithilfe der Website und der App von Blockcerts stattfinden. Zur Inspektion ist es möglich, jegliche Tools der verwendeten Blockchain zu nutzen, solange sich die Transaktion, die den Hash in die Blockchain eingetragen hat, finden lässt.

Auf der technischen Ebene unterscheidet sich Blockcerts von den bisherigen Types. Beispielsweise sind die zugrunde liegende Struktur und die Standards alle Open Source und auf Github wiederzufinden. Bei dem Blockcerts-Standard selbst handelt es sich um eine ursprünglich vom MIT Media Lab und von Learning Machine entwickelte und dann auf Open-Source-Basis publizierte Extension des Mozilla-Open-Badge-Standards.[47] Es ist also kein proprietäres Projekt, im Kontrast zu den bisher vorgestellten Types.

[46] Blockcerts: *Introduction*.
[47] IMSGlobal 2017: *cert-schema*.

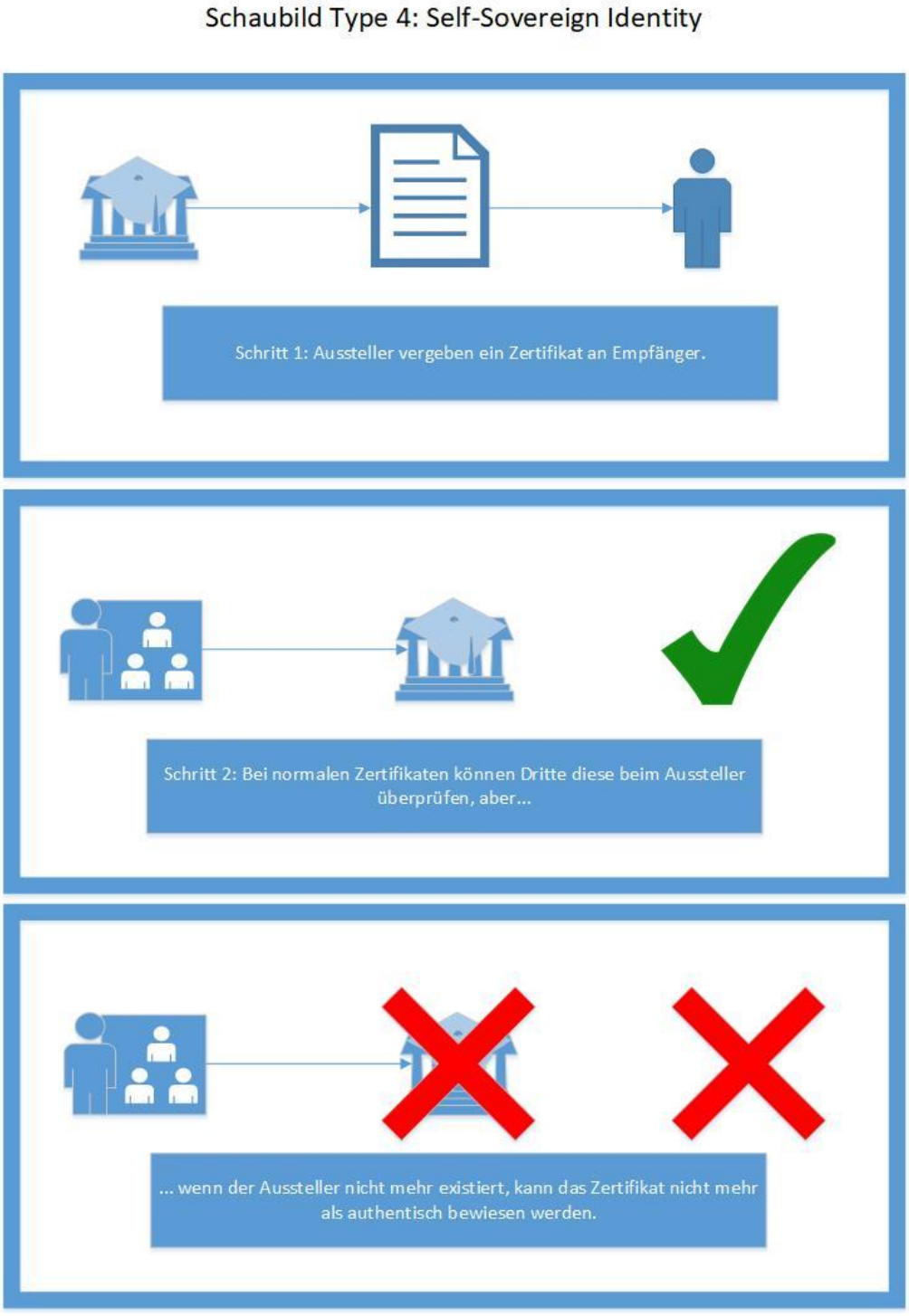


Abbildung 7: Schaubild Type 4: Self-Sovereign Identity

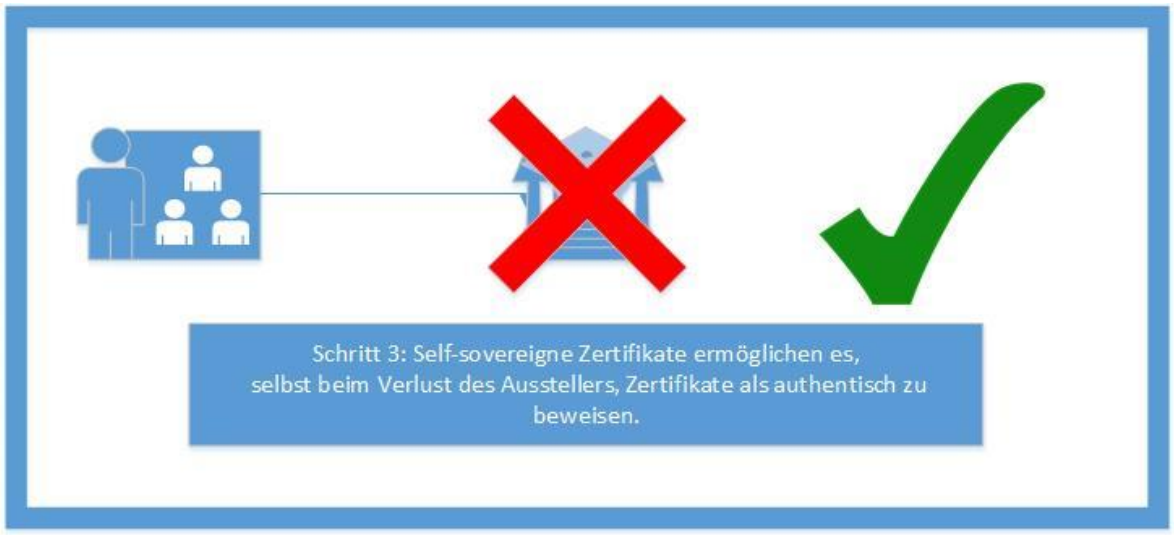


Abbildung 7 (Fortsetzung): Schaubild Type 4: Self-Sovereign Identity

5 Analyse und Vergleich

Aus den bisher vorgestellten Informationen lassen sich Schlüsse für die Analyse und die Bewertung von digitalen Zertifikaten im Bildungsbereich ziehen. Wenn wir die im zweiten Kapitel genannten Eigenschaften und Schwachstellen betrachten, können daraus wünschenswerte Kriterien hergeleitet werden:

- Niedrige **Kosten**[48]
- Hohe **Zeiteffizienz** der Prozesse[49]
- Hohe **Sicherheit** des Zertifikats[50]
- Hohe **Langzeithaltbarkeit** des Zertifikats[51]
- **Gültigkeit** des Zertifikats unabhängig vom Aussteller[52]
- Niedrige **Einstiegsbarriere** und damit eine hohe Benutzerfreundlichkeit für alle beteiligten Parteien[53]
- **Kompatibilität** mit jeglichen aktuellen Prozessen sowie gleichzeitig zukunftstauglich und technisch flexibel
- Der Grad von **Kontrolle** der Empfänger über Zertifikaten:[54] Haben Empfänger beispielsweise komplette Tragbarkeit ihrer Zertifikate, oder sind sie in der Kontrolle über ihre Zertifikate eingeschränkt?
- Die **Skalierbarkeit** muss hoch sein: Jeder Bildungsanbieter sollte idealerweise dasselbe Medium benutzen, und die Anzahl an Empfängern sollte kein Hindernis für die Umsetzung sein.
- Haben die Types besondere Eigenschaften, die zuvor nicht mit Zertifikaten verbunden worden waren? Bietet ein Type tatsächlich **Innovation**?
- Das **Zusatz**-Kriterium, in dem besondere Eigenschaften, die nicht in die anderen Kategorien passen, ebenfalls erwähnt werden können.

Diese Kriterien sind entweder Stärken und Schwächen oder wichtige Eigenschaften von analogen Zertifikaten. Unabhängig von diesen Kriterien spielen allerdings die Interessen der Entwickler selbst eine weitere Rolle. Der Kriterienkatalog wird erstellt, damit möglichst vergleichbare Kategorien zwischen den verschiedenen Types ermittelt werden können. Im Hinblick auf die vorher genannten Kriterien und Faktoren soll mithilfe einer SWOT-Analyse ein Vergleich der verschiedenen Types erstellt werden.

[48] Siehe 2.2. Aktuelle Probleme von analogen Zertifikaten, S. 3.
[49] ebd.
[50] ebd.
[51] Siehe 2.1. Eigenschaften von aktuellen, analogen Zertifikaten, S. 3.
[52] Siehe 2.2. Aktuelle Probleme von analogen Zertifikaten, S. 3.
[53] Siehe 2.1. Eigenschaften von aktuellen, analogen Zertifikaten, S. 3.
[54] Empfänger können ihr Zertifikat mit sich führen und sind nicht ortsgebunden. Sie können selbst wählen, wie und wann sie ihr Zertifikat nutzen wollen.

Die SWOT-Analyse ist ein Instrument aus dem Bereich des Unternehmenmanagements. In ihr werden die Stärken (Strengths), Schwächen (Weaknesses), Chancen (Opportunities) und Risiken (Threats) eines Unternehmens untersucht, um effektive Strategien für die Zukunft zu entwickeln. Bei den Stärken und Schwächen handelt es sich um unternehmensinterne Faktoren, während Chancen und Risiken unternehmensexterne Faktoren sind. In der vorliegenden Arbeit wird die SWOT-Analyse genutzt, um die wichtigsten Kriterien der verschiedenen Zertifizierungsmodelle fair zu untersuchen. Die Methode wird dabei auf die Inhalte der Untersuchung angepasst. Die Informationen und Kategorien, die für die Analyse benötigt werden, sollen mittels des Kriterienkatalogs eingeschränkt werden, um damit eine die Vergleichbarkeit und die Fairness während der Analyse zu erhöhen.

Ziel der SWOT-Analyse ist es, Hochschulen und weiteren öffentlichen Bildungsanbietern zu ermöglichen, erfolgreiche Strategien zur Einführung von digitalen Zeugnissen zu formulieren. Deswegen wurden vorher die Kriterien und relevanten Informationen ermittelt. Ziel dieser Analyse ist es nicht, einen genauen und kategorischen Vergleich zwischen den verschiedenen Types zu ermöglichen. Während es bei manchen Beispielen möglich ist, alle Funktionen eines Types auch öffentlich auszuführen, sind andere nur kommerziell oder bis jetzt gar nicht öffentlich zugänglich. Ein Beispiel dafür sind die Kosten. Während bei Accredible im Vendor-as-Notary-Type mit feststehenden Kosten eine genaue Kostenrechnung vorgenommen werden kann, ist das beim Know-Your-Customer-Beispiel Civic nicht möglich. Momentan wird Civic im öffentlichen Bildungsbereich nicht genutzt, sodass es auch keine genauen Zahlen zu den damit verbundenen Kosten gibt. Es können lediglich Variablen der Kosten aufgezeigt werden.

5.1 SWOT-Analyse Proof of Existence

Stärken

Kosten – Die Kosten einer Proof-of-Existence-Umsetzung hängen von mehreren Faktoren ab. Sie lassen sich in Anschaffungskosten und laufende Kosten einteilen. Die Anschaffungskosten bestehen aus den Entwicklungskosten der konkreten Umsetzung für den Anbieter und für die Integration dieser Umsetzung in bisherige Zertifikationsprozesse, den Kosten für die Weiterbildung der Mitarbeiter und Nutzer des Bildungsanbieters und den Anschaffungskosten für die Kryptowährung. Laufende Kosten entstehen durch die Hashes, die auf die Blockchain geschrieben werden müssen. Je weniger Hashes eingetragen werden müssen, desto niedriger sind auch die Kosten. Je nach Volumen und Umsetzung können diese Kosten in großem Maße variieren.

Die Kosten für eine Transaktion beispielsweise auf der Bitcoin Blockchain werden darüber berechnet, wie groß die Datenmenge der Transaktion sein wird. Je nachdem, wie viele Bitcoin auf welche Weise erworben werden und in einer Transaktion genutzt werden sollen, kann die Größe von Transaktionen variieren.[55] Die schnellsten und sichersten Transaktionskosten sind am 08.07.2018 0,00000006 BTC/byte, und die Median Transaktionsgröße liegt bei 225 byte.[56] Daraus folgt, dass die Transaktionskosten insgesamt 0,00001350 BTC betragen. Am 08.07.2018 Stand 1,0 BTC bei 6606,36 $[57], also betragen sich die Kosten für einen einzigen Hash auf ca. 0,09 $.

Wenn jedes einzelne Zertifikat separat in die Blockchain eingetragen werden soll, kommen diese Kosten auf jedes Zertifikat. Im Gegensatz dazu kann eine Umsetzung, die alle Hashes bündelt und dann nur einen Hash in die Blockchain einträgt, insgesamt diese Kosten tragen. Damit können die Kosten also veringert werden.

Sicherheit – Proof-of-Existence-Umsetzungen von digitalen Zertifikaten zeigen auf eindeutige und einfache Weise, dass Dokumente und Zertifikate über längere Zeiträume unverändert geblieben sind. Diese Sicherheit liegt in der Blockchain, die für die Umsetzung genutzt wird, begründet. In den großen und für Proof of Existence meistgenutzten Blockchains Bitcoin und Ethereum gibt es bis jetzt wenige Fälle von direkten Sicherheitsproblemen. Die Proof-of-Existence-Methode ist von den meisten Sicherheitsproblemen im Bereich von Kryptowährungen nicht betroffen, da dafür eine feindliche Übernahme der genutzten Währung stattfinden müsste. Bei den meisten und größten Hacks, die im Zusammenhang mit Kryptowährungen passiert sind, handelt es sich um Probleme und Sicherheitslücken, die nicht direkt die Sicherheit vorheriger Einträge in einer Blockchain gefährden. Die meisten Hacks und Schlagzeilen haben mit Handelsplattformen von Kryptowährungen zu tun.[58]

Skalierbarkeit – Dank des Bündelns von Hashes lässt sich diese Methode beliebig skalieren. Proof-of-Existence-Types sind unabhängig von der Größe des Bildungsanbieters und des Volumens an Zertifikaten nutzbar. Je nach Modell kann es unter Umständen keinerlei Unterschied für Bildungsanbieter und Empfänger machen, wie viele Zertifikate tatsächlich ausgestellt werden. Der Unterschied zwischen zwei Dateien, deren Hashes kombiniert werden, und 100.000 Dateien, die in einem Hash kombiniert werden, ist

[55] Bitcoin Wiki 2018: Help:FAQ.
[56] Earn: *Bitcoin Fees for Transactions.*
[57] Coinmarketcap: *Bitcoin price, charts, market cap and other metrics.*
[58] Blockgeeks: *5 High Profile Cryptocurrency Hacks*.

lediglich die Größe der Kombination.[59] In die Blockchain wird letztendlich nur ein Hash eingetragen, nämlich der Hash, der alle vorherigen Hashes sichern soll.

Zeiteffizienz – Die Hashes lassen sich unabhängig von dem Anbieter oder dem Betreiber der Infrastruktur, die sich um das Erzeugen und das Versehen mit den Hashes kümmern, digital verifizieren. Die Informationen, die zur Überprüfung benötigt werden, sind öffentlich auf der Blockchain einsehbar. Dies kann beispielsweise mithilfe eines Tools oder durch selbstständiges Teilnehmen mit einer Node am genutzten Netzwerk erreicht werden. Andererseits muss der Hash der zu überprüfenden Datei von der Partei, die die Überprüfung durchführen will, mit dem korrekten Hash-Algorithmus erzeugt werden. Auch dafür gibt es frei verfügbare Anwendungen, die automatisiert werden können. Solange der Erstellungsprozess für die digitalen Zertifikate, die gehasht werden sollen, selbst zeiteffizient designt wird, kann der Hashing-Prozess ebenfalls effizient und automatisiert in den Erstellungsprozess eingebaut werden.

Kontrolle – Je nachdem, ob die Proof-of-Existence-Umsetzung weiterhin analoge Zertifikate benutzt oder exklusiv digitale erstellt, haben die Empfänger variierende Kontrollmöglichkeiten. Wenn ein analoges Zertifikat genutzt wird und eine Datei zur Ergänzung mit Proof of Existence gesichert werden soll, behalten die Empfänger weiterhin die gewohnte Kontrolle über ihr analoges Zertifikat. Falls ein digitales Zertifikat genutzt wird, haben Empfänger ebenfalls die Kontrolle über diese Datei. Die Tragbarkeit ist insofern eingeschränkt, dass Hashes auf der Blockchain nur mit einer Internetverbindung überprüft werden können.

Die Privatsphäre von Empfängern wird insofern respektiert, dass keinerlei Daten über Empfänger gesammelt werden. Da Hashes nur in eine Richtung funktionieren,[60] sind die Informationen, die festgehalten werden, gesichert.

Kompatibilität – Die für diesen Type meistgenutzten Blockchains Bitcoin und Ethereum basieren auf Open Source[61, 62]. Deren Entwickler sind daran interessiert, so kompatibel und technisch flexibel nutzbar zu sein wie nur möglich. Je häufiger diese Kryptowährungen genutzt werden, desto größer ist sowohl der Wert als auch deren Sicherheit.

Die Entwickler von Bitcoin und Ethereum sind daran interessiert, dass diese auch von Maschinen genutzt werden können.[63] Das Internet der Dinge[64] ist ein zukünftig großer, potenzieller Markt für Nutzer von Kryptowährungen. Deswegen ist dieser Type insofern bereit für das Internet der Dinge, als es für ein Programm möglich ist, eigenständig den Hash einer Datei zu generieren, diesen mit den auf einer Blockchain festgehaltenen Werten zu vergleichen und je nach Authentizität entsprechend zu handeln.[65]

Einstiegsbarriere – Proof-of-Existence-Umsetzungen haben für Aussteller, Empfänger und Dritte eine niedrige Einstiegsbarriere. Auf einer technischen Ebene geschehen mit einer Datei, die gesichert werden

[59] Beispielsweise eine Indexdatei mit zwei oder 100.000 Einträgen.
[60] Aus einem Hash kann die originale Datei nicht erzeugt werden, aber Hashes können endlos gleich aus der originalen Datei erzeugt werden.
[61] Bitcoin 2018: *Bitcoin*.
[62] Ethereum: *Ethereum.*
[63] Kern 2017: *Blockchain soll 2018 das Internet der Dinge revolutionieren.*
[64] Das Internet der Dinge meint die zunehmende Fähigkeit von elektronischen Geräten, mithilfe des Internets und Sensoren miteinander zu kommunizieren und selbstständig und automatisch zu handeln. Mehr dazu unter: Schipper 2015: *Was eigentlich ist das Internet der Dinge?.*
[65] Stampery: *BTA Technology by Stampery.*

soll, zwei Dinge: Ein Hash der Datei wird erstellt und dieser Hash wird bei einer Transaktion auf die Blockchain geschrieben. Selbst wenn zwischen diesen beiden Schritten ein Merkle-Baum hinzugefügt wird, bedeutet dies mehr Arbeit für die Entwickler der konkreten Infrastruktur, die ein Bildungsanbieter nutzen will. Darüber hinaus ist die Nutzungserfahrung für Aussteller, Empfänger und Dritte simpel. Viele Portale dieses Types benutzen Drag-&-Drop-Menüs.[66] Wenn einmal die konkrete Umsetzung eingeführt worden ist, beschränkt sich die Wartung des Systems auf die Kompatibilität mit der restlichen technischen Infrastruktur des Bildungsanbieters, die sich im Laufe der Zeit verändern kann.

Schwächen

Kosten – Wenn die Proof-of-Existence-Umsetzung von digitalen Zertifikaten nur als zusätzliche Form der Zertifikation zur analogen genutzt wird, bleiben die Kosten für analoge Zertifikate weiterhin bestehen.

Kompatibilität – Zertifikate dürfen im Nachhinein nicht verändert werden. Wenn ein Empfänger Informationen auf einem Zertifikat hat, die er nicht teilen möchte oder die aktualisiert werden müssten, muss der Empfänger sich vom Aussteller wieder ein neues Zertifikat ausstellen lassen. Wenn es sich beispielsweise um eine Note auf einem Schulzeugnis handelt, ist es allerdings nicht möglich, von der ausstellenden Schule ein solch eingeschränktes Zeugnis zu erhalten. Es können also immer nur die Informationen geteilt werden, die auch auf dem Zertifikat festgehalten wurden.

Benutzerfreundlichkeit – Die Hashes, die auf der Blockchain öffentlich gespeichert werden, sind ohne eine Kopie der dazugehörigen Datei nutzlos. Wenn die Umsetzung nur mit einem digitalen Zertifikat gemacht wird und Empfänger die Zertifikate verlieren, hat die Methode prinzipiell keine Antwort dafür. Lösungen für dieses Problem müssen an Stellen außerhalb der Methode gefunden werden. Eine mögliche Lösung dafür wäre beispielsweise, dass der Aussteller den Empfängern permanent einen Webserver mit Kopien der Zertifikate zur Verfügung stellt. Dabei handelt es sich allerdings um eine einzigartige Lösung vonseiten des Ausstellers. Deswegen kann diese Lösung nicht allgemein zum Type gezählt werden.

Langzeithaltbarkeit – Es ist unklar, wie lange aktuelle, ausgestellte digitale Zertifikate tatsächlich nutzbar und gültig sein werden. Mit dem Fortschritt und der Veränderung von Software und Hardware werden alte Dateiformate teilweise durch neue ersetzt, oder sie werden im Laufe der Zeit weniger genutzt.[67] Insofern kann die Sicherheit eines Dokuments irrelevant sein, wenn das Dokument selbst nicht eingesehen werden kann. Deswegen ist die Effektivität des Proof-of-Existence-Types als Sicherung davon abhängig, dass das Dateiformat, in dem Zertifikate erstellt werden, eines mit hoher Zukunftstauglichkeit ist.

Für das Internet der Dinge verständlich zu sein, könnte auch eine in der Zukunft wichtige Eigenschaft für Zertifikate werden. Wenn ein Dateiformat gewählt wird, dass die Informationen des Zertifikats nicht auch maschinell lesbar macht, könnte dies dazu führen, dass diese Zertifikate bei der Suche von Maschinen benachteiligt oder ignoriert werden. Unter diesen Umständen müssten Aussteller neue Zertifikate in einem anderen Format erstellen oder anders auf diese Problematik reagieren.

Chancen

[66] Stampery: *Estonian ID Integration*.
[67] Patrizio 2014: *GIF is Dead; Long Live WebM.*

Kompatibilität – Bei Proof of Existence wird eine Datei mit einem Hash versehen und dieser Hash wird auf einer Blockchain festgehalten. Aus dieser grundlegenden Beschreibung lassen sich weitere Bereiche für die Nutzung einer Proof-of-Existence-Infrastruktur bei Bildungsanbietern ermitteln. Beispielsweise kann eine Universität die Ergebnisse von Klausuren und Hausarbeiten, die Ergebnisse von Forschung und Ideen für Patente mit einem Hash versehen. Auf diese Weise könnten durch die entsprechende Proof-of-Existence-Infrastruktur nicht nur Zertifikate eines Bildungsanbieters, sondern jegliche Dokumente, die in irgendeiner Weise nachweisbar unverändert oder mit einem Zeitstempel versehen werden müssen, gesichert werden. Auf einem niedrigeren Level könnte diese Methode auch von Studenten genutzt werden, um zu zeigen, welche Teile einer Gruppenarbeit von wem und zu welchem Zeitpunkt erstellt wurden.

Risiken

Benutzerfreundlichkeit – Diese Methode setzt teilweise eine hohe Kompetenz beim Empfänger voraus. Wenn die genutzten Zertifikate nur digital vorliegen, müssen Empfänger vollkommen selbstständig in der Lage dazu sein, auf lange Zeit wichtige Dateien zu sichern. Es gibt keinen Grund dafür, anzunehmen, dass Empfänger eher dazu in der Lage sind, dies digital zu handhaben als analog.

Kosten – Proof of Existence benutzt zum Sichern von Dateien Kryptowährungen, um Daten auf der Blockchain permanent festzuhalten. Kryptowährungen, unter anderem die beiden für diesen Type oft genutzten Bitcoin und Ethereum, haben einen rasanten und sehr volatilen Anstieg an Wert gehabt. Am 01.06.2013 war der Stand von Bitcoin bei ca. 129 $ während er am 01.06.2018 einen Wert von ca. 7,597.42 $ hat.[68] Der Höchstwert in diesem Zeitraum war ca. 19,083 $ am 19.12.2017. Bei Ethereum handelt es sich um eine Veränderung von ca 1,35 $/ETH am 01.09.2015 auf ca. 586 $/ETH am 01.06.2018 mit einem Höchstwert von ca. 1340 $/ETH am 13.01.2018.

Je nachdem, wie Bildungsanbieter an die benötigte Kryptowährung gelangen und wie sich der Markt für diese in der Zukunft entwickelt, kann es zu extrem großen Schwankungen in den Kosten für Bildungsanbieter, die diese Methode benutzen wollen, kommen.

Langzeithaltbarkeit – Meistens haben Umsetzungen dieses Types keinerlei Ausfallsicherung bei Verlust der originalen Datei. Wenn keine externe Möglichkeit besteht, eine Kopie der gesicherten Datei an anderer Stelle herunterzuladen, bedeutet der Verlust der Datei auch den endgültigen Verlust des Zertifikats.

Eine Ausfallsicherung wäre, dass der Aussteller eine Kopie der Datei für Empfänger auf eigenen Servern bereithält. Dies führt allerdings zu fortlaufenden Erhaltungskosten und verleitet die Empfänger dazu, keine eigenen Kopien der Datei zu sichern, sondern sich auf die permanent vorhandene Version des Ausstellers zu verlassen. Dies wiederum führt zu genau dem gleichen Problem, unter dem analoge Zertifikate leiden – der Aussteller und das Zertifikat gehen verloren und der Empfänger hat keine Möglichkeit mehr, seinen Bildungsabschluss mit einem Dokument nachzuweisen.

[68] Coinmarketcap: *Bitcoin price, charts, market cap and other metrics.*

5.2 SWOT-Analyse Vendor as Notary

Stärken

Kosten – Die Kosten für diesen Type lassen sich je nach kommerziellem Anbieter exakt im Voraus berechnen. Diese Systeme funktionieren oft so, dass möglichst viel automatisch und für bestimmte Gruppen insgesamt passiert. Accredible berechnet zum Beispiel die Kosten über die Anzahl an Empfängern, denen der Aussteller Zertifikate vergibt, pro Jahr:[69]

- 1.000 Empfänger pro Jahr für 80 $ pro Monat (960 $ im Jahr)
- 2.000 Empfänger pro Jahr für 150 $ pro Monat (1.800 $ im Jahr)
- 4.000 Empfänger pro Jahr für 250 $ pro Monat (3.000 $ im Jahr)
- 10.000 Empfänger pro Jahr für 500 $ pro Monat (6.000 $ im Jahr)
- Über 10.0000 Empfänger pro Jahr erhalten einen personalisierten Preis.

Kompatibilität – Accredible ist mit einem Teil der gängigen Infrastruktur, die beispielsweise in Hochschulen verwendet wird, kompatibel: Moodle, Canvas, Wordpress, Brightspace, Bridge, Microsoft Azure AD, Thinkific, Kajabi, xapiapps, Ruby on Rails und Php.[70]

Einstiegsbarriere – Die Einstiegsbarriere ist für alle Beteiligten eines Vendor-as-Notary-Type (außerhalb des Betreibers) niedrig. Hilfreiche Editoren zum Erstellen von Zertifikaten, die Möglichkeit, auch vorherige Grafiken zu importieren und zu nutzen, Drag-&-Drop-Menüs, zentralisierte Statistiken für Aussteller und eine Gruppenfunktion, um Gruppen von Empfängern zu erzeugen, machen die Bedienung für Aussteller einfach.

Skalierbarkeit – Die Skalierbarkeit ist nur durch das Budget des Ausstellers begrenzt. Accredible ist beispielsweise von Grund auf dafür entwickelt, mehrere große Gruppen zu verwalten (Gruppenfunktion) sowie Zertifikate und Badges in großer Anzahl auszustellen.

Zeiteffizienz – Alle Prozesse, die die Zertifikate involvieren, sind daraufhin entwickelt, möglichst automatisch abzulaufen, und benutzerfreundlich gestaltet. Auch das Überprüfen eines Blockchain Timestamp ist mit einem Klick zu erreichen.[71]

Zusatz – Dieser Type sollte theoretisch der am schnellsten einführbare Type sein. Aufgrund der hohen Kompatibilität von Accredible und der aktiven Entwickler, die daran interessiert sind, Kunden zu gewinnen, besteht für Accredible und weitere Anbieter die Motivation, das Produkt möglichst effizient zu liefern und funktionsfähig zu machen.

[69] Accredible: *Certificate and Badge Pricing*.
[70] Accredible: *Certificates & Badges – Accredible Integrations.*
[71] Accredible: *Example Certificate – Jordan Smith*.

Kleine Veränderungen von Zertifikaten werden von Accredible unterstützt, selbst wenn es sich dabei um mit Blockchain gesicherte Zertifikate handelt. Eine mögliche Veränderung ist beispielsweise die nachträgliche Änderung von Namen der Empfänger. Solch eine Veränderung wird deutlich im Überprüfungsprozess widergespiegelt, allerdings wird dabei auch explizit gezeigt, dass das Zertifikat selbst weiterhin gültig ist. Dies kann beispielsweise bei der Änderung von Namen anlässlich einer Heirat das erneute Ausstellen eines Zertifikats ersparen.

Schwächen

Sicherheit – Die Sicherheit dieses Types ist von der Sicherheit des Anbieters der Plattform abhängig. Darüber hinaus ist beispielsweise Accredible nicht transparent hinsichtlich seiner Methoden zur Sicherung. Aussteller und Empfänger wissen nicht, wie genau Zertifikate gesichert werden.

Zeiteffizienz – Bei technischen Problemen oder Störungen sind Empfänger und Aussteller vom Anbieter der Plattform abhängig. Je nachdem, wie viele Ressourcen der Anbieter für die Beseitigung solcher Probleme investiert, kann dies zu Problemen für Aussteller und Empfänger führen.

Langzeithaltbarkeit – Die Langzeithaltbarkeit von Zertifikaten hängt vollkommen vom Betreiber des Vendor-as-Notary-Systems ab. Falls der Betreiber des Systems nicht mehr fortbesteht, fallen auch die Zertifikate, die er betreut hat, weg.

Kosten – Je nach dem Vertrag, den der Aussteller mit dem Betreiber abschließt, und der Menge an Zertifikaten, die sie regelmäßig und zukünftig ausstellen, kann es finanziell eine wesentlich preiswertere Lösung sein, eine Alternative zu wählen.

Kontrolle – Nutzer haben nur darüber Kontrolle, mit wem sie ihr Zertifikat teilen. Die einzige Möglichkeit, Einfluss darauf zu nehmen, wer das Zertifikat einsehen darf, ist, dies privat bei Accredible zu machen. Danach kann das Zertifikat nur mithilfe des spezifischen Links gefunden werden. Nutzer haben keine Kontrolle darüber, wie und wo ihre Zertifikate gespeichert werden. Darüber hinaus sind Nutzer vollkommen darauf angewiesen, ein internetfähiges Gerät und eine mobile Internetverbindung mit sich zu führen, wenn sie die Authentizität ihres Zertifikats persönlich demonstrieren wollen.

Gültigkeit – Empfänger sind vollkommen vom Anbieter des Systems abhängig. Wenn der Anbieter des Systems schließen muss, verschwinden mit ihm auch die Zertifikate, die er bereitgestellt hat. Nach dem Schließen des Anbieters müssen Aussteller neue Zertifikate vergeben. Wenn Aussteller und Anbieter beide nicht mehr existieren, haben Empfänger keinerlei Möglichkeit mehr, vergangene Leistungen zu beweisen.

Kompatibilität – Kommerzielles Interesse kann Kompatibilität im Wege stehen. Wenn beispielsweise Moodle ein eigenes Vendor-as-Notary-System entwickelt, könnte Accredible sich dazu entscheiden, diesen Konkurrenten nicht mehr auf technischer Basis zu unterstützen. Als Konsequenz daraus könnte es zu einer Fragmentierung vonseiten der Aussteller kommen: Will beispielsweise eine Universität Moodle beibehalten und sich für eine neue Lösung für digitale Zertifikate entscheiden oder wird die Universität ein neues System anstelle von Moodle einführen, um weiterhin den gleichen Anbieter von Zertifikaten zu benutzen?

Innovation – Vendor-as-Notary-Systeme bringen grundlegend keine Innovation auf dem digitalen Zertifikationsmarkt. Zwar kann von einem Vendor-as-Notary-System Blockchain genutzt werden, aber durch die Intransparenz der Methoden eines Anbieters wird dies redundant. Wenn bei einem Zertifikat nicht die Möglichkeit besteht, den genauen Hash und die Transaktion, die den Hash auf einer Blockchain festhält, einzusehen, verschwindet die Sicherheit, die Blockchain liefern kann.

Bei einem intransparenten System vertrauen Dritte dem Anbieter des Vendor-as-Notary-Systems. Sie sind darauf angewiesen, dass der Anbieter sein Wort über zu überprüfende Zertifikate einhält. Wenn das Zertifikat gültig ist, dann vertrauen alle Beteiligten trotzdem nur der Aussage des Anbieters. Sie sind nicht in der Lage, diese Behauptung eigenständig zu überprüfen, da die genaue Datei des Zertifikats, der Hash des Zertifikats und die Transaktion, in der der Hash auf einer Blockchain festgehalten wird, nicht einzusehen sind.

Es gibt keine Beweise dafür, dass ein System, in dem das Vertrauen in die Authentizität eines digitalen Zertifikats bei einem kommerziellen Anbieter liegt, eine neue Möglichkeit ist. Was das Endprodukt angeht, wäre diese Methode, ein digitales Zertifikat anzubieten, bereits vor der Entwicklung von Blockchain und dessen Applikation in diversen Bereichen möglich gewesen. Wenn die Möglichkeit, ein solches Zertifikat anzubieten, seit mehreren Jahren existiert, warum hat sich solch ein digitales Zertifikat bis jetzt nicht etabliert? Warum kommt es jetzt – gemeinsam mit Blockchain – an den digitalen Zertifikationsmarkt? Ohne eine Untersuchung dieser Fragen lassen sich keine definitiven Schlüsse ziehen.

Allerdings lässt sich an anderer Stelle eine Beobachtung machen. In den letzten fünf bis zehn Jahren, und mit besonderer Intensität in den letzten zwei Jahren, ist der Markt an Blockchain-Produkten rasant gewachsen. Beispielsweise ist der Markt von Bitcoin von 6.473.532.037 $ am 01.01.2016 auf 117,506,606,000 $ 08.07.2018 gestiegen.[72]

Projekte wie beispielsweise Bitconnect demonstrieren, dass es möglich ist, mehrere Millionen Euro Wert an finanziellen Mitteln zu erwerben, ohne ein Produkt mit dem entsprechenden Wert zu entwickeln. Bitconnect ist eine Kryptowährung, die oft als Schneeballsystem kritisiert wurde. Nachdem Bitconnect aus rechtlichen Gründen die als Schneeballsystem kritisierte Funktion eingestellt hat, verlor der Wert der Kryptowährung von ihrem Höchststand von 17.12.2017 bei ca. 442,49 $ auf ca. 0,48 $ am 08.07.2018.[73]

Wenn die Möglichkeit, ein Vendor-as-Notary-Zertifikat zu erstellen, technisch gesehen seit Jahren besteht, kann es sein, dass die Nutzung von Blockchain hier ein taktisches Manöver zum Gewinnen von weiteren Investoren ist. Solange Blockchain in einem Projekt genutzt wird, besteht die Möglichkeit, auf der Welle von aktuellen Investitionen zu reiten. Ein Beispiel für das finanzielle Potenzial, das mit einem Blockchain-Projekt kommen kann, ist Kodak und das KodakCoin. Nach der Veröffentlichung dieses Projekts hat sich der Wert von Kodak-Aktien verdreifacht.[74] Bei Vendor-as-Notary-Zertifikaten, die technisch bereits seit längerer Zeit möglich sind und Blockchain nicht in vollem Potenzial ausnutzen, kann der Verdacht bestehen, dass es sich um ein Produkt handelt, das nur auf dieser Welle von Investitionen reiten will.

[72] Coinmarketcap: *Bitcoin price, charts, market cap and other metrics.*
[73] Rixecker 2018: *Als Schneeballsystem kritisierte Krypto-Plattform macht dicht.*
[74] Penke 2018: *Wer steckt wirklich hinter Kodak-ICO und KodakCoin?.*

Chancen

Es konnten keine Chancen für diesen Type ermittelt werden.

Risiken

Sicherheit – Bei Benutzen von einem kommerziellen Anbieter für diesen Type wird eine neue Sicherheitsschnittstelle in die Überprüfung von Zertifikaten eingeführt.

Die Sicherheit und das Vertrauen in die Zertifikate von Empfängern hängt absolut vom Anbieter und Betreiber des Systems ab. Falls der Ruf oder die Authentizität des Unternehmens infrage gestellt wird, sind alle zugehörigen Zertifikate ebenfalls infrage gestellt.

Das Vertrauen in Betreiber dieses Types steht insofern infrage, als die Prozesse und die Infrastruktur des Unternehmens oft intransparent sind. Diese Intransparenz gilt sowohl für Dritte als auch für Empfänger und Aussteller. Nur die Betreiber des Systems wissen, wie es funktioniert.

Gültigkeit – Die folgenden Konsequenzen für Aussteller und Empfänger, wenn Zertifikate plötzlich von einer dritten, kommerziellen Partei abhängen, sind unklar: Was passiert, wenn der Anbieter des Vendor-as-Notary-Systems aufgekauft wird? Was passiert, wenn der Käufer beispielsweise politisch daran interessiert ist, die Authentizität der nun aufgekauften Zertifikate infrage zu stellen, da Sicherheitslücken im System entdeckt wurden? Gemeinsam mit der Abhängigkeit von einem kommerziellen Anbieter kommen so mehrere, bis jetzt nicht existente Probleme in Betracht.

In demselben Geiste ist es auch potenziell gefährlich für Empfänger, den Anbieter des Systems, mit dem ihre Zertifikate gesichert werden, zu kritisieren. Das Nutzen eines Vendor-as-Notary-Systems für diese Aufgabe führt eine neue Machtdynamik in die Überprüfung von Zertifikaten im Bildungsbereich ein.

Langzeithaltbarkeit – Falls eine Alternative zu Vendor-as-Notary-Systemen der normale Type für digitale Zertifikate wird, könnte es zur Insolvenz der Firma führen. Unter diesen Umständen steht die Zukunft der Zertifikate wieder infrage.

Zusatz – Hackings von globalen Einrichtungen, wie beispielsweise Sonys Playstation-Netzwerk und Facebook, bei denen Millionen von Datensätzen über Personen gestohlen werden, zeigen, dass es fragwürdig ist, ob die intransparente Sicherung von wichtigen Daten und Dokumenten bei einer zentralen, kommerziellen Instanz dafür ein permanentes und sicheres Konzept darstellt. Zentralisierung führt zwangsweise zu Problemen in dieser zentralen Einrichtung. Sobald die Sicherheit und Zugriffsmöglichkeit der Zentrale infrage stehen, stehen alle davon abhängigen Funktionen ebenfalls infrage.[75] Wenn Zertifikate sich auf die Server eines Unternehmens verlassen und dieses beispielsweise unter einem Denial-of-Service[76] Angriff leidet, können die abhängigen Zertifikate dadurch unerreichbar werden. In Kombination mit der Intransparenz dieses Types können Sicherheitsprobleme ebenfalls ein Risiko sein. Wenn für Dritte nicht klar ist, wie Zertifikate gesichert werden, und das Unternehmen gehackt wird, ist die Authentizität aller Zertifikate des

[75] Dickson 2017: *Why does the centralized internet suck?*.
[76] Ein cyberkrimineller Akt, bei dem meistens die IT-Infrastruktur einer Webseite mit einer großen Menge von Aufrufen überwältigt wird. Dadurch bricht die Infrastruktur der Webseite zusammen und sie wird für Nutzer nicht mehr zugreifbar.

Anbieters infrage gestellt. Außer dem Aussteller ist niemand in der Lage, zu überprüfen, welche Zertifikate unberührt oder weiterhin authentisch sind. Insofern müssen Dritte wieder in die Aussagen des Ausstellers vertrauen. Essenziell macht es für Dritte keinen Unterschied, ob ein Vendor-as-Notary-System gehackt wurde oder nicht. Solange die Intransparenz besteht, vertrauen Dritte immer ausschließlich auf die Aussagen des Ausstellers.

5.3 SWOT-Analyse Know Your Customer

Stärken

Kosten – Das Geschäftsmodell von Know-Your-Customer-Systemen zielt darauf ab, kostenfrei für Empfänger und Aussteller zu sein.[77] Die Rolle von Überprüfern im System bietet manchen Ausstellern, beispielsweise Hochschulen, die Möglichkeit, teilzunehmen. Für die Teilnahme am System werden Überprüfer mit CVC belohnt, welches über Krypto-Handelsplattformen, wie Binance oder Coinbase, in lokale Währung umgewandelt werden kann. Auf diese Weise bieten Know-Your-Customer-Systeme eine mögliche Einkommensquelle für Bildungsanbieter an.

Sicherheit – Know-Your-Customer-Systeme nutzen oft Applikationen für Mobiltelefone. Jegliche Informationen, die dann im Know-Your-Customer-Netzwerk eingetragen werden sollen, werden nur lokal auf dem Mobiltelefon gespeichert. Auf diese Weise werden im Know-Your-Customer-Netzwerk keine privaten Informationen direkt gespeichert, sondern nur deren Validität in Form eines Hashes.[78]

Kontrolle –Empfänger haben in jedem Schritt des Prozesses die Kontrolle darüber, welche Informationen und Beweise sie teilen wollen. Darüber hinaus halten sie weiterhin die originalen Zertifikate, die sie sich von Überprüfern zukommen lassen mussten, um am System teilzunehmen. Es werden keine persönlichen Daten und Informationen direkt in das System gespeichert.

Zeiteffizienz – Empfänger müssen nur beim Erhalten neuer Zertifikate, wenn sie die Behauptungen darauf dem System hinzufügen möchten, an das System weitergegeben werden. Danach läuft alles über das System weiter. Dritte können auf einer einzigen Plattform die Behauptungen aus Bewerbungen überprüfen. Das kürzt Kosten und Arbeit des gesamten Überprüfungsprozesses.

Einstiegsbarriere – Obwohl Know-Your-Customer-Umsetzungen ambitioniert in ihren Zielen und in der Breite an Nutzern, die sie suchen, sind, ist die Nutzung solcher Systeme meistens sehr einfach. Die niedrigen oder vollkommen fehlenden Nutzungskosten für Empfänger und die hohe Benutzerfreundlichkeit (Nutzer müssen nur Informationen in die App eintragen und Zertifikate vorlegen, um die Informationen zu beweisen) sind Stärken des Systems.

Schwächen

Kosten – Zwar ist das Geschäftsmodell von Civic darauf ausgelegt, dass Empfänger dieses kostenfrei nutzen können, aber Civic verlässt sich gleichzeitig darauf, dass die Aussteller (also konkret Bildungsanbieter) vorherige Kosten tragen. Das Know-Your-Customer-System kann analoge Zertifikate nicht ersetzen. Das System zielt darauf ab, Dienstleistungen zur Identitätsfeststellung[79]zu verbessern.[80] Es zielt nicht darauf ab, die grundlegenden Zertifikate zu ersetzen, sondern darauf, den Prozess der Überprüfung und den Austausch

[77] Civic 2018: *Token Behavior Model*. S. 4.
[78] Civic 2017: *Whitepaper*. S. 12.
[79] „Als Identitätsfeststellung wird die Überprüfung bezeichnet, welche Personalien (Identität) einer natürlichen Person zuzuordnen sind, beispielsweise einem Bankkunden, der ein Konto eröffnen will." (Juraforum: *Identitätsfeststellung*.)
Dazu gehören aber allgemein alle Prozesse, in denen persönliche Informationen überprüft werden müssen, also beispielsweise auch die Überprüfung von Bewerbungsunterlagen für ein Unternehmen zur Identitätsfeststellung.
[80] Civic 2017: *Whitepaper*. S. 1.

derselben zu verbessern. Das bedeutet, dass diese Zertifikate weiterhin an anderer Stelle, in welcher Form auch immer, erstellt werden müssen. Daraus folgt, dass Aussteller weiterhin die bisherigen Kosten tragen werden.

Zeiteffizienz – Bei der ersten Angabe von Informationen vonseiten des Empfängers müssen diese Informationen weiterhin von Menschen direkt überprüft werden. Erst wenn die Informationen mit Beweisen von Personal des Überprüfers bestätigt wurden, kann die Information im System auch vom Empfänger genutzt werden.

Sicherheit – Das nötige Versenden von Beweisen und die damit einhergehende Speicherung vonseiten des Betreibers des Systems oder autorisierter Personen führt zu mehreren Lücken in der Sicherheit und Privatsphäre von Empfängern. An diesen Stellen können Informationen über Empfänger möglicherweise an nicht autorisierte Personen gelangen. Sich um die Sicherheit in diesem Schritt zu kümmern, führt unter Umständen zu weiteren Kosten und Problemen.

Das lokale Speichern von Daten auf dem Mobiltelefon des Empfängers bringt ebenfalls Probleme mit sich. Auch wenn die lokalen Daten beispielsweise kryptografisch verschlüsselt und nur mit einem Fingerabdruckscan aufgerufen werden können, so können solche Maßnahmen doch umgangen werden.

Ein weiteres Problem, das idealerweise mit digitalen Zertifikaten gelösten werden sollte, sind Krisensituationen und der Verlust von Zertifikaten, der bei solchen Situationen entstehen kann. Wenn die Behauptungen lokal und sicher auf dem Mobiltelefon des Empfängers gespeichert sind, aber ursprünglich beispielsweise auf einem analogen Zertifikat festgehalten wurden, handelt es sich um eine Situation, die weiterhin keine endgültige Lösung für das Verlustproblem ist.

Das Mobiltelefon des Empfängers muss weiterhin vollkommen funktionstüchtig bleiben und die Daten auf dem Mobiltelefon dürfen auf keine Weise beschädigt werden. Selbst wenn diese beiden Bedingungen erfüllt sind, kann der Empfänger nach dem Verlust des originalen Zertifikats nur innerhalb des Systems bezeugen, dass vorherige Behauptungen wahr sind. Insofern ist der Empfänger nach einer Krisensituation auf das System angewiesen und an dieses gebunden. Um außerhalb des Know-Your-Customer-Systems zu beweisen, dass beispielsweise der Empfänger das Abitur erreicht hat, braucht er trotzdem ein Zertifikat davon. Das Know-Your-Customer-System kann ihm in diesem Fall nicht helfen.

Die Menge an Daten, die ein Überprüfer erhält, können variieren. Beispielsweise kann nicht im System repräsentiert werden, dass die validierte Information auf der Grundlage einer qualitativ niedrigen Fotokopie stattgefunden hat, oder ob beispielsweise das Original vom Empfänger persönlich vorgezeigt wurde. Mehrere Dritte können inkorrekt validierte Informationen akzeptieren, bevor diese als inkorrekt markiert werden. Überprüfer sind nicht perfekt. Kein Überprüfer kann mit absoluter Sicherheit garantieren, dass alle seine Überprüfungen genau sind. Mithilfe von Spezialisierung auf bestimmte Typen von Daten, Anwendungsfälle oder Anforderungen von Dritten können sie allerdings ihre Genauigkeit und das Vertrauen in sich verbessern.[81]

[81] Civic 2018: *Token Behavior Model*. S. 5.

Kontrolle – Die Infrastruktur und das Format, die Know-Your-Customer-Netzwerke nutzen, sind meistens von proprietärer Natur. Bereits jetzt gibt es mehrere verschiedene Anbieter. Daten werden von verschiedenen Anbietern auf verschiedene Weisen gesichert. Da es sich um konkurrierende Plattformen handelt, gibt es keine Möglichkeit, Informationen aus einem System in das andere zu importieren – dies führt dazu, dass Empfänger und Dritte unter Umständen mehrere Know-Your-Customer-Netzwerke nutzen müssen. Insofern haben Empfänger keine Möglichkeit, ihre bestätigten Behauptungen außerhalb des Systems technisch tragbar oder gültig zu machen.

Zusatz – Es werden weiterhin Zertifikate separat vom Know-Your-Customer System benötigt. Dieser Type ist nicht dafür entwickelt worden, vollkommen andere Zertifikate zu ersetzen. Der Type ist eine Plattform, auf der die Authentizität von Behauptungen auf sichere und schnelle Weise überprüft werden kann. Es ist in Know-Your-Customer Systemen nicht möglich, direkt Zertifikate auszustellen. Wenn Empfänger Zertifikate nur in Form des Know-Your-Customer-Systems vorliegen hätten und keine weiteren besäßen, wären sie nicht mehr in der Lage, Dritten, die dieses Know-Your-Customer-System nicht nutzen, jegliche Zertifikate vorzulegen.

Damit nur ein Know-Your-Customer-System genutzt wird und keine weiteren Zertifikate mehr nötig sind, müsste jegliche Nutzung von Zertifikaten eines Empfängers auf einem einzigen System möglich sein. Damit würde das Modell für Empfänger ausreichen. Das bedeutet, dass das Modell ein komplettes Marktmonopol auf Zertifikate im Bildungsbereich besitzen müsste. Alle Bildungsanbieter müssten das System für jegliche Zertifikate benutzen, damit es nicht nötig ist, außerhalb des Systems Zertifikate zu benötigen. Jegliche Anfragen an Empfänger würden auch über dieses System laufen müssen, was bedeuten würde, dass alle Arbeitgeber das System ebenfalls benutzen müssten.

Momentan gibt es allerdings nicht nur verschiedene proprietäre Anbieter von Know-Your-Customer-Systemen, sondern auch diverse grundlegend andere Methoden, digitale Zertifikate anzubieten. Aus diesen Gründen ist es unwahrscheinlich, dass es in nächster Zeit eine Umsetzung geben wird, die eine klare Monopolstellung auf dem digitalen Zertifikationsmarkt einnehmen wird. Die Konsequenz daraus ist – selbst bei Nutzung von Know-Your-Customer-Systemen –, dass weiterhin andere Formen von Zertifikation (ob analog oder digital) benötigt werden.

Skalierbarkeit – Die Skalierbarkeit des Systems hängt davon ab, ob genug Überprüfer da sind, um die Anfragen von Dritten zu bearbeiten. Solange im System genug Überprüfer vorhanden sind, kann es so lange skaliert werden, wie das Budget zur Überprüfung es Dritten erlaubt.

Chancen

Zeiteffizienz – Je größer die Nutzung einer Know-Your-Customer-Umsetzung in einem bestimmten Rahmen ist, umso effizienter wird sie für alle Beteiligten. Am besten funktioniert Know Your Customer in einer Monopolstellung oder zumindest in einer 100%igen Nutzung in einem bestimmten Rahmen.

Wenn beispielsweise alle öffentlichen Grundschulen in einem Bundesland sich dazu bereit erklären würden, Zeugnisse für Schüler auch auf dem Know-Your-Customer-System Civic auszustellen, würde die Einführung von Civic zum Überprüfen von Zeugnissen an weiterführenden Schulen in diesem Bundesland ebenfalls Sinn machen. Wenn alle öffentlichen Grundschulen in einem Bundesland dieses System benutzen, können

folgende Bildungsanbieter das System nutzen, um Zeit und Kosten zu sparen. Da die weiterführenden Schulen in diesem Beispiel die Plattform nutzen, um Zeugnisse zu überprüfen, und damit bereits mit dem System vertraut sind, besteht die Möglichkeit, das System auch voll auszunutzen und selbst darauf weitere Zeugnisse auszustellen. Dieser Effekt könnte sich so lange wiederholen, bis Schüler den Bildungsweg verlassen und eine Arbeitsstelle suchen. Unabhängig davon, wie viele Bildungsangebote Schüler genutzt haben, macht es dann auch Sinn für Arbeitgeber, dieses System zu nutzen. In so einem System wäre es möglich, alle bisherigen Zeugnisse von Arbeitnehmern auf einer einzigen Plattform schnell und kostengünstig zu überprüfen. Diese Infrastruktur könnten auch Bildungsanbieter nutzen, womit sich das System weiter verbreiten würde.

Je früher im Bildungsweg ein solches Know-Your-Customer-System eingeführt und genutzt wird, desto mehr potenzielle Nutzung wird das System erfahren und desto mehr Sinn macht es für nachfolgende Bildungsanbieter, das System ebenfalls zu nutzen.

Im hier beschriebenen Beispiel wird zwar ein regionaler Rahmen genutzt, aber es könnte sich dabei auch beispielsweise um einen Fachbereich handeln: Wenn alle naturwissenschaftlichen oder auch nur schon die Chemie betreffenden Fachbereiche aller Hochschulen in Deutschland sich darauf einigen könnten, ein bestimmtes System für ihre Zertifikate zu nutzen, könnte dieses auch bis zu den Arbeitgebern in diesem Bereich durchdringen. Und es macht wiederum mehr Sinn für einen Arbeitgeber, solch ein System nicht nur für einen beschränkten Teil von Arbeitnehmern zu nutzen, sondern dies immer zu benutzen, wenn es möglich ist.

Innovation – Know-Your-Customer-Systeme wie Civic versuchen ein Problem zu lösen, in dem digitale Zertifikate aus dem Bildungsbereich nur eine kleine Rolle übernehmen können. „Civic is building an ecosystem that is designed to facilitate on-demand, secure and low-cost access to identity verification (‚IDV') services via the blockchain, such that background and personal information verification checks will no longer need to be undertaken from the ground up every time."[82] Es handelt sich bei Civic also um einen Anbieter, der das aktuelle Wirtschaftssystem von IDV-Dienstleistungen grundlegend verändern will.

Risiken

Zeiteffizienz – Damit Empfänger ihre Zertifikate nutzen können, müssen Dritte, die das Zertifikat überprüfen möchten, ein Geschäftspartner oder Nutzer des Know-Your-Customer-Betreibers sein. Es ist nicht möglich, Zertifikate im System außerhalb des Systems zu verifizieren. Wenn beispielsweise ein Großkonzern mit einem breiten Sortiment es Empfängern (also potenziellen Arbeitnehmern) ermöglichen will, ein System zum schnellen Bestätigen von Zertifikaten zu nutzen, muss der Großkonzern unter Umständen mehrere verschiedene Systeme nutzen, um tatsächlich allen möglichen Empfängern diese Möglichkeit zu bieten. Dies führt zu weiterer Arbeit und ist ineffizient.

Kosten und Langzeithaltbarkeit – Das Beispiel für eine Know-Your-Customer-Umsetzung in der vorliegenden Arbeit ist Civic. Bei Civic handelt es sich nicht nur um ein Know-Your-Customer-System, sondern auch um eine damit verbundene Kryptowährung. Die Kryptowährung (CVC) ist bei Civic die Währung, um die Plattform zu nutzen. Damit können Teilnehmer des Systems Preise für eigene Dienstleistungen setzen.

[82] Civic 2017: *Whitepaper*. S. 1.

Darüber hinaus ermöglicht die Währung aber auch ein ökonomisches Interesse für das ehrliche Handeln der Teilnehmer.[83]

Insofern ist die Kryptowährung ein wichtiger Teil von Civic. Trotzdem ist im letzten Jahr CVC ebenfalls Teil der Welle von volatiler Preisschwankung im Bereich von Kryptowährungen gewesen. Während am 11.08.2017 ein CVC einen Wert von bis zu ca. 0,65 $ hatte, war der niedrigste Wert zuvor 0,16 $ am 20.07.2017 und der heutige Preis beläuft sich auf ca 0,26 $ (10.06.2018).[84] Jede Plattform, die auf diese Weise versucht, Bitcoin oder Blockchains generell zu nutzen, bindet sich auch an die damit verbundenen Preisschwankungen. Auch wenn Civic im gleichen Zeitraum bei Weitem nicht so volatil ist wie beispielsweise Bitcoin, ist die Preisschwankung ein Faktor, der Einfluss auf die Wahl einer Plattform zur digitalen Zertifikation nimmt. Eine ständige Preisschwankung in den Kosten, die möglicherweise zu einem Mehrfachen der ursprünglichen Kosten anschwellen kann, und über die weder Aussteller noch Betreiber des Systems direkt eine Kontrolle haben, ist ein schwer kalkulierbarer Faktor.

[83] Civic 2018: *Token Behavior Model*. S. 6.
[84] Coinmarketcap: *Civic (CVC) price, charts, market cap, and other metrics.*

5.4 SWOT-Analyse Self-Sovereign Identity

Stärken

Zusatz – Es gibt wenig Konkurrenten auf dem self-sovereignen Zertifikationsmarkt. Interessierte können einen umfassenden Überblick in diesem Bereich bekommen und sich so eine genauere Meinung über die Umsetzungen bilden.

Bei Blockcerts handelt es sich nicht um einen kommerziellen Anbieter, sondern um einen offenen Standard. Blockcerts vertritt keine kommerziellen Interessen und ist mittlerweile vollkommen ein Open-Source-Projekt. Learning Machine und das Massachusetts Institute of Technology (MIT) waren an der Entwicklung von Blockcerts beteiligt, allerdings ist es mittlerweile ein öffentlicher Standard. Das Dienstleistungsangebot von Learning Machine besteht darin, Software zum Ausstellen von Blockcerts auf einer großen Skala anzubieten, nicht aber den Standard selbst.[85]

Kompatibilität – Self-Sovereign-Identity-Umsetzungen sind generell teilweise oder komplett Open-Source-basiert.[86] Auf diese Weise können Entwickler von Ausstellern bereits vor der Einführung eines solchen Systems damit experimentieren und überprüfen, ob und wie sehr die Umsetzung zur technischen Umgebung des Ausstellers passt. Teil dieser Projekte ist es auch, mit offenen Standards, wie beispielsweise dem Mozilla-Open-Badges-Standard und weiteren W3C-Standards, kompatibel zu sein.

Es besteht kein Interesse daran, auf einer bestimmten Blockchain exklusiv Zertifikate zu sichern, und dank der Open-Source-Natur dieser Art von Projekten besteht die Möglichkeit, auf mehreren verschiedenen Blockchains Zertifikate zu sichern.[87]

Sicherheit – Unabhängig davon, was mit dem Aussteller des Zertifikats passiert, kann ein self-sovereignes Zertifikat so lange seine Authentizität demonstrieren, wie die Blockchain, auf der es gesichert wurde, weiter besteht. Da ökonomisches Interesse für Besitzer und Miner daran besteht, dass mehrere dieser Blockchains in Form von öffentlich zugänglichen Kryptowährungen weiter bestehen und Wert haben, ist die Zukunft von self-sovereignen Zertifikaten insofern sicher.

Kosten – Die einzigen laufenden Kosten sind Transaktionskosten, mit denen Hashes auf eine Blockchain geschrieben werden. Diese Kosten unterscheiden sich, je nach Wahl der Blockchain und der Art der genauen Umsetzung. Bei einem Blockcerts-Zertifikat, das mit Bitcoin gesichert werden soll, können die zuvor berechneten Kosten[88] für eine Transaktion genutzt werden. Etwa 0,09 $ pro Zertifikat. Wobei diese Kosten bei größeren Bündeln von Zertifikaten weiter gesenkt werden können, beispielsweise bei einer Anzahl von 100 Zertifikaten auf etwa 3 $.[89]

Einstiegsbarriere – Empfänger haben volle Kontrolle über ihre Zertifikate. Bei den Zertifikaten selbst handelt es sich um Dateien. Diese können von Empfängern zur Sicherung an mehreren verschiedenen Orten kopiert

[85] Smolenski 2018: *Top 10 Reasons to Use Blockcerts.*
[86] ebd.
[87] ebd.
[88] Siehe 5.1 SWOT-Analyse Proof of Existence, S.27.
[89] Kim 2017: *Issuing options*.

und gespeichert werden, sodass einem kompletten Verlust der Datei vorgebeugt werden kann.[90] Insofern ist ein Zertifikat vollkommen tragbar und an kein spezifisches Gerät gebunden.

Im Kontrast zu anderen Types hat Blockcerts eine niedrigere Einstiegsbarriere. Empfänger müssen lediglich ein mit Blockcerts kompatibles Wallet[91] herunterladen und können ihr Zertifikat in vollem Umfang nutzen.

Langzeithaltbarkeit – Blockcerts wird mit etablierten, offenen Standards aufgebaut. Dabei werden Dateiformate genutzt, von denen sich eine lange Haltbarkeit erhofft wird, im Kontrast zu beispielsweise proprietären Dateiformaten von weiteren kommerziellen Anbietern.

Kontrolle – Im Kontrast zu anderen Types von digitaler Zertifikation, die ebenfalls Blockchain nutzen, enthält ein Zertifikat vom Self-Sovereign-Identity-Type die persönliche Blockchain-Adresse des Empfängers und die des Ausstellers. Es ist für einen Dritten klar und deutlich, welche Blockchain-Transaktion genau sein Zertifikat auf der Blockchain festgehalten hat. Die Identität des Empfängers ist in das Zertifikat selbst mit eingebaut. Sowohl Aussteller als auch Empfänger können zu einem späteren Zeitpunkt auf eine andere Form von Zertifikaten umsteigen, aber sie haben eine weiterhin bestehende Kontrolle über ihr Blockcerts-Zertifikat.[92]

Schwächen

Einstiegsbarriere – Empfänger übernehmen die volle Verantwortung für ihre eigenen Zertifikate. Sie müssen darüber aufgeklärt werden, dass das konkrete Zertifikat nur eine Datei ist. Die Datei muss von ihnen ähnlich sicher behandelt werden, wie heute mit analogen Originalen umgegangen wird. Die Möglichkeiten ein self-sovereignes Zertifikat zu sichern, müssen von Empfängern proaktiv wahrgenommen werden. Bei Verlust der Datei ist das Zertifikat verloren. Auch wenn dies bei der Entwicklung der Umsetzungen berücksichtigt wird, besteht trotzdem die Gefahr des endgültigen Verlusts.

Wenn von einem öffentlichen Bildungsanbieter keine analoge Alternative zu Blockcerts angeboten wird, benötigen Empfänger zwangsweise elektronische Geräte, die ihm die Möglichkeit geben, das Zertifikat zu benutzen und zu verwalten. Dazu gehören auch moderne Smartphones, wobei Heimcomputer aber besser geeignet sind.[93] Eine Internetverbindung wird ebenfalls zwangsweise benötigt, um ein Zertifikat aktuell überprüfen zu können.

Die Komplexität, mit einem solchen Zertifikat verantwortungsvoll umzugehen und permanent dem endgültigen Verlust vorzubeugen, ist anspruchsvoll. Während sich öffentliche Einrichtungen in diversen Bereichen mit digitaler Langzeitarchivierung auseinandersetzen, ist auf individueller Ebene nur eingeschränktes Interesse vorhanden.[94, 95] Persönliche Langzeitarchivierung von Daten ist weiterhin ein komplexes und bis jetzt nicht zuverlässig gelöstes Problem.

[90] Smolenski 2018: *Top 10 Reasons to Use Blockcerts.*
[91] Als Wallets werden Programme oder Webseiten bezeichnet, in denen Kryptowährungen gespeichert und verwaltet werden können.
[92] ebd.
[93] Heimcomputer fallen nicht aus der Hand, können schwerer verloren gehen, Windows und MAC eignen sich weiterhin besser für komplexe Prozesse als auf Android basierende Smartphones oder ein iPhone.
[94] Marshall, Catherine C 2006: *The Long Term Fate of Our Digital Belongings: Toward a Service Model for Personal Archives,* S.6.
[95] ebd.

Chancen

Kosten – Anders als bisherige Types können self-sovereigne Zertifikate potenziell analoge Zertifikate im Bildungsbereich komplett ersetzen. Ein starkes Argument gegen analoge Zertifikate sind die damit eingehenden hohen Kosten pro Zertifikat. Mit diesem Type könnten diese Kosten permanent wesentlich gesenkt werden.

Kompatibilität – Aufgrund der Open-Source–Struktur von Blockcerts und ähnlichen Umsetzungen besteht das Potenzial, dass alle self-sovereignen Zertifikate mit den meisten technischen Umgebungen kompatibel gemacht werden können.

Risiken

Langzeithaltbarkeit - Es ist noch unklar, wie gut skalierbar und langzeitbeständig dieser Type tatsächlich ist. Zwar gibt es verschiedene Experimente dieses Types, allerdings befinden sich diese in einem – im Vergleich zu anderen Types – relativ jungen Stadium und Zeitraum.

5.5 Gegenüberstellung der Zertifizierungsmodelle

Im Hinblick auf die verschiedenen Types von digitalen Zertifikaten lassen sich zwei verschiedene Tendenzen erkennen: Entweder sie werden parallel zu analogen Zertifikaten ausgestellt und erweitern somit die Möglichkeiten, das Zertifikat frei zu nutzen. Oder sie zielen darauf ab, analoge Zertifikate zu ersetzen. Ergänzungen zu analogen Zertifikaten sind Proof-of-Existence- und Know-Your-Customer-Modelle, während Vendor-as-Notary- und Self-Sovereign-Identity-Modelle versuchen, analoge Zertifikate zu ersetzen.

Welche Strategie gewählt wird, hängt von den Rahmenbedingungen des Bildungsanbieters ab. Basierend auf aktuellen Informationen und den digitalen Zertifikaten auf dem Markt, lassen sich nur eingeschränkte Schlüsse ziehen. Deswegen kann es für einen Bildungsanbieter auch gerechtfertigt sein, keine Entscheidung zu treffen und darauf zu warten, dass sich auf dem regionalen oder auf dem für ihn relevanten Markt ein klares Modell durchsetzt. Bildungsanbieter, denen so ein Verhalten zu empfehlen sein könnte, sind beispielsweise Grundschulen, denen die finanziellen Mittel und das Personal fehlen, einen potenziellen Umstieg auf ein neues Zertifikationsmodell in Angriff zu nehmen.

Kosten – Alle Anbieter von digitalen Zertifikaten bieten die Möglichkeit, in einem kleinen, kostengünstigen und meist sogar freien Rahmen die Umsetzung zu testen und kennenzulernen. Ebenso teilen alle Formen von digitalen Zertifikaten, dass die Einführung in die technische Umgebung eines Bildungsanbieters ein komplexer Prozess ist. Der Arbeitsaufwand, um die verschiedenen Formen von Zertifikaten konkret zu testen und die Kompatibilität mit der genutzten technischen Umgebung einzelner Bildungsanbieter zu überprüfen, kann potenziell sehr variieren. Insofern unterscheiden sich die damit verbundenen Kosten ebenfalls. Dazu kommen noch Erklärungen und Tutorials, wie genau die neue Form von Zertifikaten in voller Funktion genutzt werden kann, da es sich bei diesen Systemen um bisher fremde Prozesse handelt.

Je nachdem, ob eine Umsetzung eine Alternative zu oder ein Ersatz von analogen Zertifikaten sein soll, verändern sich die Kosten entsprechend. Know-Your-Customer- und Proof-of-Existence-Umsetzungen sind darauf angewiesen, dass weiterhin separate Zertifikate ausgestellt werden. Wenn es sich um analoge Zertifikate handelt, die parallel zu Know-Your-Customer- und Proof-of-Existence-Systemen erstellt werden, bleiben die Kosten für diese analogen Zertifikate weiterhin bestehen. Bei einer Know-Your-Customer-Umsetzung fallen keine weiteren Kosten für Aussteller oder Empfänger an, da ein solches System sich über eine andere Quelle finanziert. Bei einer Proof-of-Existence-Umsetzung skalieren sich die Kosten direkt mit der Anzahl an Hashes, die auf eine Blockchain eingetragen werden. Die konkrete Anzahl der Hashes und die Kosten hängt also vollkommen davon ab, wie genau die Umsetzung diesen Schritt unternimmt. Falls es sich beispielsweise um eine Universität handelt, die alle Zertifikate, die sie ausstellt, einmal pro Semester in einem einzigen Merkle-Baum zusammenbringt und dann auf eine Blockchain schreibt, entstehen geringe Kosten. Wird jeder Hash einzeln auf die Blockchain geschrieben, folgen hingegen höhere Kosten.

Die genutzten Zertifikate müssen nicht zwangsweise in analoger Form vorliegen. Ob analoge oder digitale Zertifikate genutzt werden, hängt von der Umsetzung ab. Wenn es sich allerdings um digitale Zertifikate handelt, die für Know-Your-Customer- und Proof-of-Existence-Systeme erstellt werden, macht es für Aussteller wenig Sinn, diese Types zu nutzen. Know-Your-Customer- und Proof-of-Existence-Types eignen sich dazu, die Funktionalität von analogen Zertifikaten zu erweitern und zu ergänzen.

Wenn ein Bildungsanbieter ohnehin digitale Zertifikate nutzen will, bietet es sich an, eine Umsetzung zu wählen, die versucht, analoge Zertifikate vollkommen zu ersetzen, wie Vendor-as-Notary- oder Self-Sovereign-Identity-Types. Die Kosten für Vendor-as-Notary-Types sind die Kosten, die sich vor der Einführung eines solchen Systems am genauesten berechnen lassen, da Anbieter dieser Systeme vorher in der Lage sind, alle nötigen Prozesse und Kosten zu offenbaren. Die hohe Kompatibilität dieser Systeme und das kommerzielle Interesse von Anbietern, neuen Kunden technisch entgegenzukommen, ermöglichen es den Ausstellern, genau zu berechnen, welche Kosten mit einem Umstieg auf ein Vendor-as-Notary-System anfallen würden.

Daneben stehen Self-Sovereign-Identity-Types, die mit nur sehr geringen Kosten verbunden sind. Das Erstellen einer Identität (also einer Adresse) und Transaktionen, um Zertifikate zu sichern, sind die einzigen anfallenden Kosten.

Fazit: Um wirklich Kosten zu sparen, müssen digitale Zertifikate analoge Zertifikate ersetzen und nicht nur erweitern. Nur zwei der hier vorgestellten Types ersetzen analoge Zertifikate: Vendor-as-Notary- und Self-Sovereign-Identity-Types. Vendor-as-Notary-Types zielen darauf ab, einen schnellen und reibungslosen Umstieg zu ermöglichen, der mit höheren Kosten verbunden ist als andere Types. Self-Sovereign-Identity-Types kommen mit niedrigeren Kosten aus, allerdings kann das Einführen und Anpassen an die technische Umgebung des Ausstellers mit mehr Arbeit verbunden sein – außer dieser Schritt wird ebenfalls von einem kommerziellen Anbieter gelöst, wobei hier die Kosten variieren können.

Zeiteffizienz – Alle Formen von digitaler Zertifikation zielen darauf ab, möglichst zeiteffizient zu sein. Falls das System entscheidet, eine Blockchain zu nutzen, können nur von den Entwicklern der Blockchain Probleme an dieser bearbeitet werden.

Proof-of-Existence-Types sind die zeiteffizienteste Umsetzung von digitalen Zertifikaten. Die gesamte Funktionsbreite dieser Umsetzung kann automatisiert werden und innerhalb von wenigen Minuten bis Sekunden ablaufen. Mögliche Probleme für die Zeiteffizienz liegen in der Erstellung der für den Type benötigten Dateien.

Vendor-as-Notary-Types haben die zusätzliche Schwäche, dass bei technischen Störungen Aussteller und Empfänger keinerlei Einfluss auf das Beseitigen dieser Probleme nehmen können. Darum muss sich der Betreiber eines Systems kümmern.

Know-Your-Customer-Types sind in ihrer Zeiteffizienz genauso eingeschränkt wie Vendor-as-Notary-Types; bei Problemen hat nur der Betreiber des Systems die Möglichkeit, diese zu beheben. Darüber hinaus kommt unter Umständen eine weitere Einschränkung hinzu: Nur solange ausreichend Überprüfer im System präsent sind, um den Bedarf an Überprüfungen von Dritten zu decken, kann dieser Prozess problemlos ablaufen. Je nachdem, wie umfangreich die Überprüfung ist, welche Informationen vom Empfänger bereitgestellt werden können und wie lange dieser Prozess dauert, kann sich die Dauer der Überprüfung verlängern.

Bei Self-Sovereign-Identity-Types ist das Einführen und Ausstellen von Zertifikaten ein möglicherweise komplexerer Prozess als bei Proof-of-Existence-Types, da hierfür erst einmal die benötigte Software-Umgebung voll funktionsfähig gemacht werden muss. Der Überprüfungsprozess findet aber sehr ähnlich

statt, da auf die gleiche Weise die Authentizität von Dateien gesichert wird, wie bei Proof-of-Existence-Types.

Fazit: Types, die analoge Zertifikate benutzen, sind zeitlich wesentlich ineffizienter als die Types, die versuchen, ausschließlich digital zu arbeiten. Mit analogen Zertifikaten fällt auch zwangsläufig deren Überprüfung an, und diese muss wiederum zwangsläufig von Menschen vorgenommen werden. Trotzdem ist Proof of Existence darüber hinaus die zeiteffizienteste Methode, da die nötigen Arbeitsschritte alle automatisiert werden können und simpel sind. Zertifikate vom Self-Sovereign-Identity-Type sind ähnlich zeiteffizient, vor allem da keine analogen Zertifikate vorhanden sind. Insofern besteht das Potenzial für Self-Sovereign-Identity-Types, noch zeiteffizienter als Proof-of-Existence-Types zu sein, allerdings muss zuvor das System vollkommen funktionsfähig gemacht werden – was Zeit für den Aussteller kostet. Vendor-as-Notary-Types sind ebenfalls schnell, da alles digital ablaufen kann. Es besteht allerdings eine Abhängigkeit gegenüber dem Betreiber des Systems, wenn Probleme zu lösen sind. Know-Your-Customer-Types leiden an den beiden Schwächen der analogen Überprüfung und der Abhängigkeit vom Anbieter des Systems, wenn Probleme zu lösen sind. Nichtsdestotrotz kann die Überprüfung in diesem Type schneller vonstattengehen als bei analogen Zertifikaten, da – mit vertrauten Überprüfern – die Ergebnisse der Überprüfung nicht jedes Mal wiederholt werden müssen, sondern nur dann, wenn Dritte einen neuen Überprüfer wollen.

Insgesamt sind alle digitalen Zertifikate zeitlich wesentlich effizienter als analoge Zertifikate, wenn sie einmal eingeführt sind und aktiv genutzt werden. Die größte Quelle für zeitliche Verzögerungen, das Überprüfen durch Personal, kann von ihnen im Laufe der Nutzung massiv gekürzt oder komplett entfernt werden.

Sicherheit – In den Optionen der Sicherheit unterscheiden sich die verschiedenen Types hauptsächlich hinsichtlich der Komponente, in der die Sicherheit des digitalen Zertifikats liegt. Proof-of-Existence- und Self-Sovereign-Identity-Types setzen auf die Sicherheit einer Blockchain.

Vendor-as-Notary-Types setzen auf die Sicherheit, die der Betreiber des Systems anbietet. Dabei handelt es sich teilweise auch um mit Blockchain gesicherte Zertifikate. Solange aber die Einsicht in ein solches System und die genauen Informationen, wie ein spezifisches Zertifikat gesichert wurde, unklar sind, ist dieser Prozess intransparent und aufgrund dessen schwer weiter zu bewerten.

Know-Your-Customer-Types setzten auf die Ehrlichkeit der Überprüfer im System und die bestehende Authentizität von Zertifikaten, bevor diese in das System selbst aufgenommen wurden.

Proof-of-Existence- und Self-Sovereign-Identity-Types setzten darauf, dass die ausgewählte Blockchain ungehackt bleibt. Bis jetzt gibt es noch keinen Fall einer solchen Übernahme bei den meistens dafür genutzten Blockchains Bitcoin und Ethereum. Zu beachten sind allerdings Quantencomputer die – auch wenn sie in den nächsten zehn bis zwanzig Jahren möglicherweise noch nicht so weit kommen werden – das Potenzial besitzen, aktuelle Methoden der Kryptografie, auf denen Blockchains wie Bitcoin und Ethereum heute basieren, obsolet zu machen.[96]

Fazit: Proof-of-Existence- und Self-Sovereign-Identity-Types verlassen sich auf Blockchains für ihre Sicherheit. Bis jetzt konnten die oft für diese Types genutzten Blockchains frei von Sicherheitsproblemen

[96] Teich 2017: *Quantum Computing Will Not Break Your Encryption, Yet.*

bleiben, die die bestehende Sicherheit von ausgestellten Zertifikaten infrage stellen würden. Im Gegensatz dazu müssen Vendor-as-Notary-Umsetzungen erst noch von ihrer Sicherheit überzeugen. Es gibt viele Einrichtungen, die zentralisiert Daten und Dokumente Nutzern gegenüber intransparent sichern und trotzdem gehackt werden. Die Sicherheit in Know-Your-Customer-Umsetzungen hängt von den Überprüfern im System ab. Es liegen noch nicht genügend Daten vor, um diese Sicherheit im Vergleich zu den anderen Types stichhaltig zu bewerten.

Langzeithaltbarkeit – Proof-of-Existence-Zertifikate weisen mehrere verschiedene Faktoren auf, die alle berücksichtigt werden müssen, um die Langzeithaltbarkeit eines solchen Zertifikats zu bewerten: Welches Dateiformat wird genutzt? Handelt es sich bei der Datei selbst um eine Abbildung eines analogen Zertifikats oder um ein digitales Zertifikat, das gesichert werden soll? Welche Blockchain wird zur Sicherung benutzt? Jede dieser Fragen ist eine potenzielle Quelle für mit diesem Type gesicherte Zertifikate, ihre Langzeithaltbarkeit zu verlieren.

Bei Vendor-as-Notary-Types ist das Fortbestehen der Zertifikate an das Fortbestehen des Anbieters gebunden. Anbieter können eingeschränkte Maßnahmen dagegen einführen. Beispielsweise kann bei der Übernahme des Anbieters durch eine andere Firma mithilfe einer zwingenden Vertragsklausel garantiert werden, dass alle bis zu diesem Zeitpunkt ausgestellten Zertifikate weiterhin unterstützt und instand gehalten werden müssen. Trotzdem kann nicht in allen Fällen, wie beispielsweise der Insolvenz des Anbieters, diesem Problem komplett vorgebeugt werden.

Know-Your-Customer-Types teilen diese Schwäche gegenüber dem Anbieter des Systems, allerdings handelt es sich im Kontrast zu Vendor-as-Notary-Types um ein kleineres Problem. Know-Your-Customer-Types hängen nicht komplett vom Anbieter ab, da dieser Type sich auf Zertifikate, die außerhalb des Systems erstellt werden, verlässt. Mit dem Anbieter gehen lediglich die erweiterten Funktionen des Systems verloren, während die originalen Zertifikate weiterhin erhalten bleiben. Insofern ist die Langzeithaltbarkeit von Know-Your-Customer-Types auch die Langzeithaltbarkeit der genutzten Originale.

Zertifikate in Self-Sovereign-Identity-Umsetzungen basieren auf offenen Standards und langlebigen Dateiformaten. Sie werden mit dem expliziten Ziel entwickelt, langlebig und flexibel zu sein. Die einzige Abhängigkeit, die sie vom Design her haben, besteht gegenüber der Blockchain, auf der die Zertifikate gehasht werden. Darüber hinaus sind die größte Gefahren, neben dem permanenten Verlust des Zertifikats und seiner Funktionen, Fehler vonseiten des Empfängers. Diesem kann allerdings sowohl vonseiten des Ausstellers als auch vonseiten des Empfängers vorgebeugt werden, indem mehrere gesicherte Kopien des originalen Zertifikats angefertigt werden und separat voneinander gesichert werden.

Fazit: Je größer die kommerzielle Beteiligung am Zertifikationsprozess und je mehr ein Type versucht, analoge Zertifikate nicht zu ersetzen, desto mehr Problemfaktoren kommen auf die Langlebigkeit eines Zertifikats zu. Das langiebigste Zertifizierungsmodell ist das mit offenen und unabhängigen Standards, da die

wenigsten Abhängigkeiten bestehen und eine einzige Lösung für alle offenen Umsetzungen übertragbar ist.[97]

Gültigkeit – Proof-of-Existence-Types verlassen sich auf Zertifikate außerhalb des Systems. Daraus folgt, dass die Zertifikate vom Aussteller des Zertifikats abhängig sind. Vendor-as-Notary-Zertifikate sind, wie unter dem Aspekt der Langzeithaltbarkeit bereits beschrieben, vom Fortbestehen des Anbieters des Systems abhängig. Dies betrifft auch die Gültigkeit. Know-Your-Customer-Types verlassen sich wie Proof-of-Existence-Types auf externe Zertifikate. Hier gilt das Gleiche wie bei diesen Zertifikaten: eine Abhängigkeit gegenüber dem Aussteller.

Self-Sovereign-Identity-Types sind von der Blockchain, mit der das Zertifikat gesichert wird, abhängig. Sie sind vom Aussteller unabhängig in ihrer Authentizität überprüfbar. Das sichere Fortbestehen der genutzten Blockchain ist also für Self-Sovereign-Identity-Types entscheidend.

Fazit: Self-Sovereign Identity ist der einzige Type von digitalen Zertifikaten, der es Empfängern ermöglicht, unabhängig von anderen im Zertifikationsprozess beteiligten Einrichtungen und Parteien, authentische Zertifikate zu besitzen. Die anderen Types verwenden Zertifikate, die – wie analoge Zertifikate bis jetzt – vom Aussteller abhängig sind.

Einstiegsbarriere – Die Einstiegsbarriere bei allen digitalen Zertifikaten ist im Vergleich zu analogen Zertifikaten erhöht. Um digitale Zertifikate zu überprüfen, werden ein internetfähiges Gerät wie ein Mobiltelefon oder ein PC und eine Internetverbindung benötigt.

Proof-of-Existence-Types beruhen auf technischer Ebene auf einem simplen Prozess: Empfänger können selbst mithilfe von Drag-&-Drop-Menüs die Datei, die das Zertifikat sein soll, mit einem Hash versehen, und dieser wird dann auf die Blockchain geschrieben. Dritte müssen den vorhandenen Hash der Datei mit dem Hash, der die Sicherung sein soll, vergleichen und damit ist die Authentizität geklärt.

Je nachdem, wer die Proof-of-Existence-Umsetzung betreibt und anbietet, unterscheidet sich der Arbeitsaufwand für den Aussteller. Wenn der Aussteller selbst die Aufgabe übernimmt, muss ein automatisierter Hashing-Zwischenschritt in den Erstellungsprozess von Zertifikaten eingebaut werden. Ein anderer Anbieter kann diese Aufgabe auch übernehmen.

Vendor-as-Notary-Types haben die niedrigste Einstiegsbarriere für Empfänger. Hier benötigen Empfänger nichts weiter als eine persönliche E-Mail-Adresse, die mit ihrem digitalen Zertifikat verbunden wird. Sobald diese Verbindung besteht, haben Empfänger Zugriff und Kontrolle über ihr Zertifikat. Aussteller müssen ebenfalls nur auf der Website des Anbieters ein Konto anlegen und können dort mithilfe von Tools Zertifikate erstellen und vergeben.

Know-Your-Customer-Types haben eine im Vergleich zu Proof of Existence ähnlich niedrige Einstiegsbarriere für Empfänger, da diese lediglich Zertifikate an Überprüfer senden müssen und die restlichen Funktionen des Systems über eine zentrale App ablaufen. Eine weitere Einstiegsbarriere besteht insofern, als Aussteller

[97] Wenn beispielsweise JSON-Dateien von Blockcerts in ein anderes Dateiformat geparst werden, muss nur ein einziges Mal solch ein Programm öffentlich zugänglich gemacht werden und alle von diesem Problem Betroffenen können dieses Programm nutzen, um das Problem zu beseitigen.

weiterhin Zertifikate ausstellen müssen. Dritte müssen ebenfalls Nutzer des Know-Your-Customer-Systems werden, damit das System genutzt werden kann.

Self-Sovereign-Identity-Types haben insofern die höchste Einstiegsbarriere, als es für Empfänger wichtiger ist, Zertifikate eigenverantwortlich zu speichern und zu lagern. Dies ist ein größeres Problem als beispielsweise bei Proof-of-Existence-Types, da die Intention von Self-Sovereign-Identity-Types darin besteht, den Empfänger und sein Zertifikat Ausstellern gegenüber unabhängig zu machen. Wenn allerdings Empfänger sich durch eigenes Verschulden in eine Lage bringen, in der sie den Zugriff auf eigene Zertifikate verlieren, kann dies unter Umständen in einer Situation geschehen, in der der Aussteller keine weitere Kopie davon mehr ausstellen kann. Deswegen ist es essenziell wichtig, dass sowohl Empfänger kompetent genug sind, eigene Zertifikate auf lange Zeit zu sichern, als auch, dass das System für den eventuellen Verlust von Zertifikaten vorbeugende Maßnahmen besitzt, die nicht vom Aussteller abhängig sind.

Aufseiten der Aussteller kann der Arbeitsaufwand bei der Nutzung von Self-Sovereign-Identity-Types variieren. Je nachdem, wie sehr die vorhandene Software für die technische Umgebung des Ausstellers personalisiert werden muss, steigt der Arbeitsaufwand. Für Dritte handelt es sich, wie bei Proof of Existence, um eine kurze Überprüfung von zwei Hashes.

Fazit: Alle Umsetzungen von digitalen Zertifikaten zielen darauf ab, möglichst niedrige Einstiegsbarrieren zu haben. Während sie alle die gleichen technischen Einstiegsbarrieren teilen (Hardware, Internet, Check gegen eine Blockchain), haben Vendor-as-Notary-Types die insgesamt niedrigste Einstiegsbarriere für alle Beteiligten. Danach folgen Proof-of-Existence- und Know-Your-Customer-Types. Die größte Einstiegsbarriere kann für DSS-Umsetzungen bestehen, was aber nicht bedeutet, dass das auch immer so sein muss. Dies kommt auf den konkreten Kontext einer Situation an, da viele Faktoren auf die Situation einwirken. Hauptfaktoren sind hier die technische Umgebung des Ausstellers und ob das nötige Personal vorhanden ist, um den Type einzuführen und voll funktionsfähig zu machen.

Kompatibilität – Alle Zertifikate, die sich auf die Sicherung einer Datei mithilfe eines Hashes, der auf eine Blockchain festgeschrieben wird, verlassen, können – was die technischen Anforderungen betrifft – einen automatisierten und maschinenfreundlichen Überprüfungsprozess anbieten. Außer bei Vendor-as-Notary-Umsetzungen kann bei den anderen Types die konkrete Blockchain, die genutzt werden soll, vom Aussteller gewählt werden.

Proof-of-Existence-Types sind grundlegend mit allen Dateiformaten und selbst mit analogen Zertifikaten kompatibel. Da sich dieser Type auf Zertifikate von außerhalb verlässt, gehen aktuelle Prozesse nicht durch die Nutzung von Proof of Existence verloren.

Vendor-as-Notary-Umsetzungen sind insofern sehr kompatibel mit aktuellen Systemen wie Moodle, als es im Interesse der Anbieter dieser Systeme liegt, die Umsetzung attraktiv und einfach in Prozesse von Ausstellern einbaubar zu machen. Mehrere gängige Arbeitsprozessmanagementsysteme sind zum Beispiel mit Accredible kompatibel. Wenn Vendor-as-Notary-Umsetzungen eigenständig funktionieren, können sie allerdings auch ohne eine direkte Integration in die bisherige technische Umgebung von Ausstellern genutzt werden. Eine große Schwäche von Vendor-as-Notary-Types ist es jedoch, nicht mehr analog oder offline ein aktuelles Zertifikat mit sich führen zu können. Darüber hinaus kann das kommerzielle Interesse des Anbieters der technischen Kompatibilität des Systems entgegenstehen.

Know-Your-Customer-Types verlieren wie Proof-of-Existence-Types keine ursprünglichen Prozesse von bisher genutzten Zertifikaten, da das System weiterhin auf diese angewiesen ist. Und da die Umsetzung an sich nicht direkt in bisherige Prozesse eingebaut werden soll, sondern ein separates System ist, bildet die Kompatibilität hier wirklich die Einstiegsbarriere für alle Beteiligten. Insofern ist ein Know-Your-Customer-System vollkommen kompatibel, wenn eine Person oder Einrichtung das System auch nutzt.

Self-Sovereign-Identity-Zertifikate sind wie Vendor-as-Notary-Zertifikate abhängig von elektronischen Geräten und dem Internet, um überprüfbar zu sein. Anders als bei Vendor-as-Notary-Umsetzungen kann allerdings kein kommerzielles Interesse der technischen Kompatibilität von Digital-Self-Sovereign-Zertifikaten entgegenstehen, da es sich bei diesen meistens um Open-Source-Umsetzungen handelt. Selbst wenn dieses System zu einem bestimmten Zeitpunkt mit einer Software nicht kompatibel sein sollte, ist es unter Umständen für Interessierte möglich, diese Inkompatibilität aufzuheben und zu beseitigen.

Fazit: Self Sovereign Identity und Proof of Existence haben die größte Kompatibilität der Umsetzungen, da es sich um offene Software handelt, die problemlos personalisiert werden kann, um auf die jeweiligen Umstände einer Einrichtung zu passen. Know Your Customer folgt mit einem System, das bisherige Zertifikate erweitert und nicht ersetzt – und gleichzeitig unabhängig von diesen funktioniert. Vendor as Notary kann die kompatibelste Umsetzung sein, falls beispielsweise ein Aussteller Moodle oder ähnliche Arbeitsprozessmanagementsysteme benutzt. Falls dies nicht der Fall ist, stehen potenzielle Vendor-as-Notary-Kunden möglicherweise vor einem Kompatibilitätsproblem, da nicht alle verschiedenen Systeme unterstützt werden.

Kontrolle – Proof-of-Existence-Umsetzungen funktionieren nur mithilfe einer Datei. Diese Datei kann das Zertifikat selbst sein oder auch eine Repräsentation eines analogen Zertifikats in der Form eines Scans. Insofern haben Empfänger die Kontrolle über die Tragbarkeit ihres Zertifikats. Auf der Blockchain werden weiterhin keine persönlichen Informationen gespeichert, lediglich unpersönliche Hashes.

Bei Vendor-as-Notary-Umsetzungen werden Zertifikate beim Anbieter des Systems gespeichert. Bei Accredible zum Beispiel besteht die einzige Kontrolle, die Nutzer über ihre Zertifikate haben, darin, ob ihr Zertifikat öffentlich zugänglich sein soll, oder ob nur die Personen, die über den Link zum Zertifikat verfügen, dieses einsehen können.

Know-Your-Customer-Umsetzungen verlassen sich wie Proof of Existence auf externe Zertifikate. Je nachdem, was ein Empfänger überprüfen lassen will, muss er dem Überprüfer bestimmte Beweise liefern. Wenn der Überprüfer die Behauptungen des Zertifikats daraufhin bestätigt hat und die Informationen im Know-Your-Customer-System festgehalten wurden, haben Empfänger die volle Kontrolle darüber, mit wem und wie sie die festgehaltenen Informationen teilen wollen.

In einer Self-Sovereign-Identity-Umsetzung haben Empfänger die komplette Kontrolle über ihr Zertifikat.

Fazit: Self-Sovereign-Identity-Umsetzungen bieten Empfängern die größte Kontrolle über ihre Zertifikate. Proof of Existence kann die bisherigen Vorteile von analogen Zertifikaten beibehalten, da diese am ehesten für den Type genutzt werden. Bei Know-Your-Customer-Types sieht dies ähnlich aus, allerdings besteht hier eine Gefahr des Kontrollverlusts, ausgehend von Überprüfern im System. Wenn Überprüfer bestimmte Informationen haben wollen, sind Empfänger unter Umständen gezwungen, Informationen und Dokumente

zu teilen, die sie eigentlich nicht teilen wollen. Bei Vendor-as-Notary-Umsetzungen haben Empfänger nur eine eingeschränkte Kontrolle über ihre Zertifikate.

Skalierbarkeit – Proof of -Existence erlaubt Skalieren, insofern die Geschwindigkeit der Blockchain, die genutzt wird, mithalten kann[98]. Aus mehreren Gründen, wie zum Beispiel Kosten und Sicherheit, macht es allerdings Sinn, Hashes, die auf die Blockchain geschrieben werden sollen, miteinander in Form eines Merkle-Baums oder beispielsweise einer Indexdatei zu bündeln und dann auf die Blockchain zu schreiben. Auf diese Weise lässt sich diese Methode fast grenzenlos skalieren.

Vendor-as-Notary-Umsetzungen lassen sich so weit skalieren, wie es der Anbieter der Umsetzung erlaubt. Falls es sich nicht um einen Sprung, der den vorbereiteten Rahmen des Anbieters überschreitet, handelt, sollte es für Anbieter kein Problem sein, das System unbeschränkt zu skalieren.[99]

Die Skalierbarkeit des Know-Your-Customer-Systems Civic hängt davon ab, wie viele Überprüfer zur Verfügung stehen und ob die Anzahl der Überprüfer groß genug ist, um die Anzahl von Zertifikaten, die überprüft werden müssen, zu bearbeiten.

Self-Sovereign-Identity-Zertifikate können ebenso wie Proof-of-Existence-Zertifikate fast unendlich skaliert werden. Die Skalierbarkeit ist an die Geschwindigkeit der Blockchain und an die damit verbundenen Kosten gebunden.

Fazit: Alle digitalen Zertifikationsmethoden haben das Potenzial, grenzenlos weiter skaliert zu werden. Am einfachsten zu skalieren ist Proof of Existence. Dort muss nur wenig Arbeit geleistet werden, um potenziell fast endlos viele Zertifikate gleichzeitig zu sichern. Know Your Customer ist eingeschränkt und abhängig von dem Verhältnis zwischen Überprüfern und deren Arbeitsaufwand. Der Self-Sovereign-Identity-Type ist mit Einschränkungen der Blockchain und dazugehörigen Kosten verbunden.

Innovation – Bei diesem Kriterium handelt es sich darum, was die jeweiligen Umsetzungen tatsächlich neu machen und neu anbieten. Alle digitalen Zertifikate teilen, dass sie elektronisch tragbar und kontrollierbar sind.

Proof of Existence ist, technisch gesehen, seit der Veröffentlichung von Bitcoin möglich. Wirklich sicher ist es aber erst mit dem großen Marktwachstum der vergangenen zwei Jahre geworden. Mit zunehmender Nutzung der Blockchain hat auch die verbrauchte Energie und damit die Sicherheit vorheriger Einträge zugenommen. Die Innovation, die diese Nutzung von Blockchain ermöglicht, besteht darin, zu zeigen, dass eine Datei über einen bestimmten Zeitraum unverändert geblieben ist.

Vendor-as-Notary-Umsetzungen bringen keine Innovation mit sich. Es ist bereits seit Jahrzehnten möglich, ein Vendor-as-Notary-System von digitalen Zertifikaten zu erstellen. Blockchain wird in Vendor-as-Notary-Systemen genauso genutzt wie in einer Proof-of-Existence-Umsetzung, allerdings ist beispielsweise bei Accredible die Nutzung von Blockchain insofern irrelevant, als die Authentizität von Accredible unabhängig von der tatsächlichen Datei bestätigt wird und nicht von einer anbieterunabhängigen Blockchain.

[98] Williams-Grut 2017: *A Bitcoin civil war is threatening to tear the digital currency in 2 — here's what you need to know.*
[99] Accredible: *Certificate and Badge Pricing*.

Tatsächlich umgesetzte Know-Your-Customer-Systeme existieren bereits in anderen Bereichen, wie zum Beispiel dem Finanzwesen. Die Know-Your-Customer-Umsetzung von digitalen Zertifikaten versucht im Fall von Civic etwas grundlegend Neues: Mithilfe von Blockchain soll ein ganzes Wirtschaftssystem von Identifikationsdienstleistungen entstehen. Dabei liefert Blockchain, in Form der Kryptowährung CVC, hier die Währung des Systems.

Self-Sovereign-Identity-Zertifikate versuchen ein weiteres grundlegendes Problem von analogen Zertifikaten zu beseitigen: die Abhängigkeit des Empfängers vom Aussteller eines Zertifikats. Diese Abhängigkeit soll permanent beseitigt werden, indem stattdessen Blockchain an diese Stelle tritt. Auf technischer Ebene erreicht dieses Ziel auch Blockcerts.

Fazit: Proof-of-Existence-, Know-Your-Customer- und Self-Sovereign-Identity-Types bringen mithilfe von Blockchain vollkommen neue Ideen und Veränderungen für Zertifikate. Self-Sovereign Identity geht am weitesten, um analoge Zertifikate zu ersetzen und bisherige Schwächen technisch zu beseitigen. Know Your Customer versucht ein fundamental neues Wirtschaftssystem aufzubauen, aktuellen Zertifikaten einen Platz darin zu geben und nicht analoge Zertifikate redundant zu machen. Proof of Existence erweitert ebenfalls aktuelle Zertifikate, allerdings in einem viel eingeschränkteren Rahmen als die anderen Types. Lediglich das unveränderte Fortbestehen einer Datei wird mit hier ermöglicht. Vendor-as-Notary-Types bringen außer der digitalen Form keine technische Innovation mit sich.

Zusatz – Über digitale Zertifikate hinaus bietet der Proof-of-Existence-Type eine Palette an verschiedenen Nutzungspotenzialen bei den Ausstellern, wie in der entsprechenden SWOT-Analyse beschrieben.[100]

Vendor-as-Notary-Types haben das Potenzial, am schnellsten von einem Aussteller einführbar zu sein. Dieser Type kann vollkommen eigenständig, ohne eine technische Integration beim Aussteller, in voller Funktionsfähigkeit genutzt werden. Darüber hinaus sind nachträgliche Veränderungen an Zertifikaten möglich. Vendor-as-Notary-Types sind allerdings auch mit einem Risiko verbunden. Große Mengen an persönlichen Daten und Dokumenten wurden immer wieder und auf verschiedene Weisen gehackt. Ein zentraler Anbieter von Zertifikaten könnte ebenfalls das Opfer von solchen Angriffen werden.

Know-Your-Customer-Types funktionieren am effektivsten als Erweiterung zu analogen Zertifikaten. Auf technischer Ebene ist es möglich, für diesen Type analoge Zertifikate vollkommen zu ersetzen, allerdings sind die Rahmenbedingungen, die dafür entstehen müssten, aktuell eher unwahrscheinlich.

Self-Sovereign-Identity-Types basieren auf offenen Standards und Open Source. Dazu kommt, dass die Anzahl von verschiedenen Umsetzungen dieses Types überschaubar ist. Insofern kann sich jeder Interessierte einen guten Überblick über diesen Type verschaffen.

Fazit: Die verschiedenen Informationen, die nicht direkt einer der vorher dargestellten Kategorien zugeordnet werden können, heben weitere Unterschiede der Types hervor.

[100] Siehe 5.1. SWOT-Analyse Proof of Existence, S. 27.

	PoE	VaN	KYC	SSI
Kosten	Kosten für analoge Zertifikate bestehen weiterhin. Kosten für einzelne Nutzungen sind niedrig und können mit entsprechender Infrastruktur weiter runtergetrieben werden.	Die teuerste Variante von digitalen Zertifikaten. Kosten können im Voraus berechnet werden.	Kosten für analoge Zertifikate bestehen weiterhin. Kostenlose Nutzung für Empfänger und Aussteller.	Kosten für analoge Zertifikate sind vollkommen abgeschafft. Geringe Kosten für einzelne Zertifikate, vergleichbar mit PoE vergleichbar.
Zeiteffizienz	Aus analogen Zertifikaten Dateien zu erstellen kann zeitineffizient sein. Am zeiteffizientesten, da die wenigste Arbeit benötigt wird.	Technische Störungen können nur vom Betreiber des Systems behoben werden.	Technische Störungen können nur vom Betreiber des Systems behoben werden. Der nötige Überprüfungsprozess muss von Menschen vorgenommen werden.	Die Einführung und Nutzung ist etwas umständlicher und komplexer als PoE. Ansonsten allerdings ähnlich effizient wie PoE, da die Arbeitsschritte fast identisch sind.
Sicherheit	Sicherheit hängt von einer Blockchain ab.	Sicherheit hängt vom Anbieter des Systems ab.	Sicherheit hängt von den Überprüfern und dem Design des Systems ab.	Sicherheit hängt von einer Blockchain ab.
Langzeithaltbarkeit	Eine Vielzahl von potenziellen Risikofaktoren besteht für die Zukunft der Zertifikate. Es besteht großes kommerzielles Interesse am Fortbestehen der genutzten Blockchains.	Die Langzeithaltbarkeit hängt komplett vom Fortbestehen des Anbieters ab.	Die Langzeithaltbarkeit hängt vom Anbieter ab. Bei Verlust des Anbieters besitzen Empfänger trotzdem vorherige Zertifikate.	Es besteht großes kommerzielles Interesse am Fortbestehen der genutzten Blockchains. Die Grundlage des Types ist Open-Source-entwickelt und kann von allen Nutzern wenn nötig verändert werden.
Gültigkeit	Zertifikate sind vom Aussteller abhängig. Die Funktionen des Types sind von der genutzten Blockchain abhängig.	Zertifikate sind komplett vom Anbieter abhängig.	Zertifikate sind vom Aussteller abhängig. Die Funktionen des Types sind vom jeweiligen Anbieter abhängig.	Zertifikate sind von der genutzten Blockchain abhängig.
Einstiegsbarriere	Die Arbeitsschritte zur Nutzung sind simpel. Der Type ist auch sehr nutzerfreundlich und einfach umsetzbar. Die Nutzerfreundlichkeit hängt immer von der konkreten Umsetzung ab und kann sehr breit variieren.	Die niedrigste Einstiegsbarriere für alle Beteiligten. Die volle Funktionalität ist beim Anbieter per Webseite möglich – von der Erstellung bis zur Überprüfung.	Nach VaN-Zertifikaten die nächstniedrigere Einstiegsbarriere. Alle Funktionen laufen über eine App des Anbieters. Die Überprüfung kann das einzige potenzielle Hindernis sein.	Die Arbeitsschritte sind teilweise so simpel wie die von PoE. Es ist essenziell für Empfänger, verantwortlich mit ihren Zertifikaten umzugehen, ansonsten kann es leicht zum Verlust derselben kommen.
Kompatibilität	Mit allen Dateiformaten kompatibel.	Kompatibilität hängt vom Anbieter ab.	Technisch unabhängig von der technischen Umgebung des	Open-Source und offene Standards bilden die technische

	Je nach genutztem Dateiformat variierend maschinell lesbar. Analoge Zertifikate können beibehalten werden.	Umsetzungen können auch vollkommen eigenständig genutzt werden, ohne Integration in die bisherige technische Umgebung des Ausstellers.	Ausstellers. Analoge Zertifikate können beibehalten werden.	Grundlage. Falls die Umsetzung nicht bereits kompatibel mit der Umgebung des Ausstellers ist, müssen Aussteller diese selbst entwickeln.
Kontrolle	Empfänger haben Kontrolle über die genutzte Datei und, wenn genutzt, das analoge Original.	Für den Empfänger besteht nur die Kontrolle, die der Anbieter erlaubt.	Empfänger haben Kontrolle über ihr Zertifikat und jegliche Informationen, die im System festgehalten werden.	Empfänger haben komplette Kontrolle über ihr Zertifikat.
Skalierbarkeit	Skalierbarkeit kann mithilfe eines Hash-Baums grenzenlos gemacht werden. Geringe Kosten, unabhängig von der Anzahl an Zertifikaten.	Skalierbarkeit ist nur vom Budget des Ausstellers eingeschränkt.	Skalierbarkeit hängt von der Anzahl an Überprüfern im System ab.	Ähnlich wie PoE grenzenlos skalierbar. Kosten sind höher als bei PoE.
Innovation	Ursprünglich eine neue Methode zur Sicherung von Daten mithilfe von Bitcoin.	Keine innovative Methode.	Nutzt Blockchain zur Erstellung eines neuen Wirtschaftssystem.	Mithilfe von Blockchain sollen Zertifikate ihre Gültigkeit unabhängig vom Aussteller beweisen können.
Zusatz	Potenzial, beispielsweise von Universitäten auch außerhalb von Zertifikaten zur Sicherung von weiteren Dokumenten, wie Hausarbeiten und wissenschaftlichen Projekten, genutzt zu werden.	Nachträgliche Veränderung von Zertifikaten ist eingeschränkt möglich. Theoretisch der Type, der am schnellsten von Ausstellern in voller Funktion genutzt werden kann. Sicherheitsrisiko durch Zentralisation wichtiger Dokumente bei einem intransparenten Anbieter.	Braucht zwangsweise externe Zertifikate.	Es handelt sich um kein Produkt, sondern offene und frei nutzbare Software.

Tabelle 1: Fazit Tabelle

Legende: Vorteile Nachteile neutrale Eigenschaften

6 Fazit und Ausblick

Der noch im Entstehen befindliche und ständig weiter wachsende Markt an verschiedenen digitalen Zertifikaten zeigt, dass Bildungsanbieter sich immer mehr bewusst werden, dass analoge Zertifikate in der Zukunft nicht mehr ausreichend sein werden. Im Hinblick auf die Frage: „Welche Formen digitaler Zertifikationen können zukünftig die analoge Zertifikation im Bildungsbereich ersetzen?“ wurde ermittelt, dass es zwei verschiedene Ansätze von digitalen Zertifikaten gibt. Eine Strategie ist, analoge Zertifikate komplett zu ersetzen. Der Vendor-as-Notary-Type und der Self-Sovereign-Identity-Type gehören diesem Ansatz an. Die andere Strategie besteht darin, analoge Zertifikate nur teilweise zu ersetzen und mit einem digitalen System ihre Funktionalität zu ergänzen. Die beiden Types Proof of Existence und Know Your Customer setzen auf diesen Ansatz.

Nach der Untersuchung der verschiedenen Types mithilfe des Kriterienkatalogs und einer SWOT-Analyse erweist sich der Self-Sovereign-Identity-Type von digitalen Zertifikaten als der Type, der die meisten der aufgestellten Kriterien am besten erfüllt. Self-Sovereign-Identity-Zertifikate setzen sich vor allem in einer Hinsicht von ihrer Konkurrenz ab: der vom Aussteller unabhängigen Gültigkeit der Zertifikate. Die Stärkung der Unabhängigkeit und Kontrolle der Empfänger durch Self-Sovereign-Identity-Zertifikate steht im Einklang mit den Aufgaben und Zielen von öffentlichen Bildungsanbietern. Die Zertifikate dieses Types

- bauen auf offenen Standards auf,
- zielen nicht darauf ab, kommerzielle Interessen zu vertreten,
- sollen auf lange Zeit flexibel nutzbar bleiben und
- sind mit wesentlich niedrigeren Kosten verbunden.

Unter Berücksichtigung der Aufgabe von öffentlichen Bildungsanbietern lässt sich der Self-Sovereign-Identity-Type klar als derjenige identifizieren, der analoge Zertifikate bei öffentlichen Bildungsanbietern ersetzen sollte.

Trotzdem konnte die Ausgangsthese: „Digitale Zertifikate des Self-Sovereign-Identity-Types werden (in den nächsten fünf bis zehn Jahren) die am weitesten verbreitete Alternative zu analogen Zertifikaten im Bildungsbereich sein.“ nicht belegt werden.

Inwiefern diese Form von Zertifikaten sich in der Zukunft bei Bildungsanbietern durchsetzen kann, konnte aufgrund von fehlenden Daten nicht untersucht werden. Ebenso haben die anderen Types von digitalen Zertifikaten eigene Stärken, sodass sie bei der Untersuchung aus einer anderen Perspektive als der von öffentlichen Bildungsanbietern eine bessere Alternative als der Self-Sovereign-Identity-Type darstellen könnten.

Was aber aus der erstellten Analyse klar wird, sind die verschiedenen Methoden der einzelnen Types und ihre größten Stärken. Proof-of-Existence-Umsetzungen nutzen eine technische Infrastruktur, die auch in weiteren Arbeitsbereichen von Bildungsanbietern genutzt werden kann. Vendor-as-Notary-Zertifikate ermöglichen es, analoge Zertifikate sofort abzulösen und dadurch Kosten zu minimieren. Know-Your-Customer-Umsetzungen zielen über den Bildungsbereich hinaus darauf ab, ein Wirtschaftssystem auf einer Plattform zu vereinen. Alle Types sind mit niedrigeren Kosten und ihrer allgemeinen digitalen Kompatibilität aktuellen analogen Zertifikaten wesentlich voraus.

Was die angewandten Methoden der vorliegenden Arbeit betrifft, wurde im Laufe der Analyse klar, dass die Kriterien etwas zu grob gefasst waren. Dies war auch damit verbunden, dass die Informationen, aus denen Schlüsse gezogen wurden, auf verschiedenen Umfängen und Quellen basierten. Bei manchen konnten direkt Zahlen vom Anbieter übernommen werden, während bei anderen nicht das gesamte Konzept greifbar war.

Öffentliche Bildungsanbieter können die vorliegende Arbeit selbst nutzen, um eigenständig Experimente mit den verschiedenen Types von digitalen Zertifikaten durchzuführen. In einem eingeschränkten Rahmen können alle Types frei oder mit wenigen Kosten verbunden getestet werden. Somit können öffentliche Bildungsanbieter, selbst mit eingeschränkten Mitteln und Ressourcen, die für sie unter den gegebenen Umständen passende Umsetzung finden.

Bildungsanbieter, die sich bis jetzt nicht mit dem Thema digitale Zertifikate auseinandergesetzt haben, sollten dies mittlerweile tun. Es besteht die Möglichkeit, Empfänger mit zukunftsrobusten und flexiblen digitalen Zertifikate auszustatten. Der Trend zur Digitalisierung findet weiterhin bereichsübergreifend statt. Momentan besteht die Chance für öffentliche Bildungsanbieter, den zukünftigen Kurs von digitalen Zertifikaten mit ihrer Wahl aktiv zu beeinflussen. Ob und wie diese Möglichkeit zukünftig umgesetzt wird, hängt von den Entscheidern der Bildungsanbieter ab.

7 Literaturverzeichnis

Letzter Zugriff auf die aufgelisteten Quellen erfolgte am 06.08.2018

Accredible. *Certificate and Badge Pricing*. Online: accredible.com. https://www.accredible.com/pricing/

Accredible. *Certificates & Badges – Accredible Integrations*. Online: accredible.com. https://www.accredible.com/integrations/

Accredible. *Example Certificate – Jordan Smith*. Online: credential.net. https://www.credential.net/10000005

Accredible. *What is a group?*.Online: accredible.com. https://help.accredible.com/hc/en-us/articles/115001155409-What-is-a-group-

Bitcoin Wiki. *Help:FAQ*. Online: bitcoin.it, 2018. https://en.bitcoin.it/wiki/Help:FAQ#How_much_will_the_transaction_fee_be.3F_.2F_Why_is_the_fee_so_high.3F

Bitcoin. *Bitcoin*. Online: github.com, 2018. https://github.com/bitcoin/bitcoin

Blockcerts. *Introduction*. Online: blockcerts.org. https://www.blockcerts.org/guide/

Blockgeeks. *5 High Profile Cryptocurrency Hacks*. Online: blockgeeks.com. https://blockgeeks.com/guides/cryptocurrency-hacks

Botschaft der Bundesrepublick Deutschland Beirut. *Merkblatt zur Legalisation syrischer Urkunden*. Online: diplo.de, 2017, S. 2. https://beirut.diplo.de/blob/2024876/a347e65b24e34a5f44b80319a0a2f845/legalisation-syr-merkblatt-deutsch-data.pdf

Civic. *Token Behavior Model*. Online: civic.com, 2018, S. 4-6. https://www.civic.com/wp-content/uploads/2018/05/Token-Behavior-Model-May-16-2018.pdf

Civic. *Whitepaper*. Online: civic.com, 2017, S. 1, 12-14 https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

Codecademy. *About Points, Badges, and Streaks*. Online: codecademy.com. https://help.codecademy.com/hc/en-us/articles/115003050088-About-Points-Badges-and-Streaks

Coinmarketcap. *Bitcoin price, charts, market cap and other metrics*. Online: coinmarketcap.com. https://coinmarketcap.com/currencies/bitcoin/#charts

Coinmarketcap. *Civic (CVC) price, charts, market cap, and other metrics*. Online: coinmarketcap.com. https://coinmarketcap.com/currencies/civic/

Dickson, Ben. *Why does the centralized internet suck?*. Online: bdtechtalks.com, 2017. https://bdtechtalks.com/2017/10/27/why-does-the-centralized-internet-suck/

Digiconomist. *Bitcoin Energy Consumption Index*. Online: digiconomist.net. https://digiconomist.net/bitcoin-energy-consumption

Durant, Elizabeth. *Digital Diploma debuts at MIT*. Online: mit.edu, 2017. http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

Earn. *Bitcoin Fees for Transactions*. Online: earn.com. https://bitcoinfees.earn.com/

English, S. Matthew. *The Path to Self-Sovereign Identity*. Online: github.com, 2017. https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

Estonian Police and Border Guard Board. *Application for e-Residency*. Online: gov.ee. https://apply.gov.ee/

Ethereum. *Ethereum*. Online: github.com. https://github.com/ethereum/

Gladstone, Jennifer. *Fake University Degrees Rampant in India*. Online: ebiinc.com, 2015. https://www.ebiinc.com/resources/blog/fake-university-degrees-rampant-in-india

Grech, Alexander; Camilleri, Anthony F. *Blockchain in Education*. Luxemburg: Europäische Union, 2017, S. 27-28. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf
Hamilton Duffy, Kim; Smolenski, Natalie. *The Time for Self-Sovereign Identity is Now.* Online: medium.com, 2017. https://medium.com/learning-machine-blog/the-time-for-self-sovereign-identity-is-now-222aab97041b

IMSGlobal. *cert-schema*. Online: github.com, 2017. https://github.com/IMSGlobal/cert-schema

Jagers, Chris. *Digital Identity and the Blockchain.* Online: medium.com, 2017. https://medium.com/learning-machine-blog/digital-identity-and-the-blockchain-10de0e7d7734

Jagers, Chris. *The New Blockcerts Mobile App*. Online: medium.com, 2018. https://medium.com/learning-machine-blog/the-new-blockcerts-mobile-app-eea18053f526

James, Riley. *Creating an immutable audit trail on the blockchain with Xero & Tierion*. Online: xero.com, 2018. https://devblog.xero.com/creating-an-immutable-audit-trail-on-the-blockchain-with-xero-tierion-be423d39380b

Juraforum. *Identitätsfeststellung*. Online: juraforum.de. https://www.juraforum.de/lexikon/identitaetsfeststellung

Kern, Ekki. *Blockchain soll 2018 das Internet der Dinge revolutionieren.* Online: t3n.de, 2017. https://t3n.de/news/blockchain-2018-eco-885681/

Kim. *Issuing options*. Online: blockcerts.org, 2017. https://community.blockcerts.org/t/issuing-options/28

Lee, Sunny; Otto, Nate. *Verifiable Claims Use Cases.* Online: w3c.github.io, 2018. https://w3c.github.io/vc-use-cases/

Lemieux, Victoria. *A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation.* Vancouver: The University of British Columbia, 2017, S. 4-8. https://www.researchgate.net/publication/322511343_A_typology_of_blockchain_recordkeeping_solutions_and_some_reflections_on_their_implications_for_the_future_of_archival_preservation/references

Marshall, Catherine C.; Bly, Sara; Brun-Cottan, Francoise. *The Long Term Fate of Our Digital Belongings: Toward a Service Model for Personal Archives*. Society for Imaging Science and Technology, 2006, S.6. https://arxiv.org/ftp/arxiv/papers/0704/0704.3653.pdf

Mehrain, Thessy. *Blockchain Enabled Self-Sovereign Identity*. Online: b-hive.eu, 2016. https://b-hive.eu/news-full/2016/11/14/blockchain-enabled-self-sovereign-identity

Orcutt, Mike. *How secure is blockchain really?*. Online: technologyreview.com, 2018. https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

Originstamp. *Free trusted timestamping*. Online: originstamp.org. https://originstamp.org/home

Passwordgenerator.net. *SHA256 Hash Generator*. Online: passwordgenerator.net. https://passwordsgenerator.net/sha256-hash-generator/

Patrizio, Andy. *GIF is Dead; Long Live WebM*. Online: smartbear.com, 2014. https://smartbear.com/blog/test-and-monitor/gif-is-dead-long-live-webm/

Penke, Michael. *Wer steckt wirklich hinter Kodak-ICO und KodakCoin?*. Online: gruenderszene.de, 2018. https://www.gruenderszene.de/allgemein/kodak-ico-ryde-startup-marke

Radenbach, Wolfgang. *Elektronische Zeugnisse und Verifikatio*. Göttingen: Universität Göttingen, 2018, S. 13, 28. www.uni-goettingen.de/de/document/download/4b91f96282e972d500f44fbdf4ef3845.pdf/elektrzeugnisse_radenbach.pdf

Rixecker, Kim. Bitconnect. *Als Schneeballsystem kritisierte Krypto-Plattform macht dicht*. Online: t3n.de, 2018. https://t3n.de/news/bitconnect-schneeballsystem-bcc-kurssturz-913642/

Schipper, Lena. *Was eigentlich ist das Internet der Dinge?*. Online: Frankfurter Allgemeine, 2015. http://www.faz.net/aktuell/wirtschaft/cebit/cebit-was-eigentlich-ist-das-internet-der-dinge-13483592.html

Smolenski, Natalie. *Top 10 Reasons to Use Blockcerts*. Online: medium.com, 2018. https://medium.com/learning-machine-blog/top-10-reasons-to-use-blockcerts-ec7d29f2712c

Stampery. *BTA Technology by Stampery*. Online: stampery.com. https://stampery.com/tech

Stampery. *Estonian ID Integration*. Online: stampery.com. http://www.stampery.com/estonia

Teich, Paul. *Quantum Computing Will Not Break Your Encryption, Yet*. Online: forbes.com, 2017. https://www.forbes.com/sites/tiriasresearch/2017/10/23/quantum-will-not-break-encryption-yet/#79eac1837319

Verband Deutscher Papierfabriken. *Pro-Kopf-Verbrauch von Papier, Karton und Pappe im internationalen Vergleich im Jahr 2012 (in Kilogramm je Einwohner)*. Online: Verband Deutscher Papierfabriken, 2014. https://de.statista.com/statistik/daten/studie/5959/umfrage/verbrauchsmenge-von-papier-in-ausgewaehlten-laendern/

Williams-Grut ,Oscar; Price, Rob. *A Bitcoin civil war is threatening to tear the digital currency in 2 — here's what you need to know*. Online: businessinsider.de, 2017. https://www.businessinsider.de/bitcoins-hard-fork-bitcoin-unlimited-segregated-witness-explained-2017-3?r=US&IR=T

Yadav ,Pankhuri. *Gang of forgers sold 50,000 school and univ degrees, set up fake websites*. Neu-Delhi: The Times of India, 2018. https://timesofindia.indiatimes.com/city/delhi/gang-of-forgers-sold-50000-school-and-univ-degrees-set-up-fake-websites/articleshow/62701357.cms

8 Anhang

Anhang 1: E-Mail der TH Koeln

Studierenden- und Prüfungsservice T 1805-00251

Sehr geehrter Herr Lubszczyk,

ein zentrales Register gibt es nicht zur Überprüfung von Abschlusszeugnissen. Deutsche Unternehmen stellen die von uns ausgestellten Unterlagen normalerweise nicht in Frage. Manchmal erhalten wir Anfragen von Organisationen z.B. WES (https://www.wes.org/), die im Auftrag von ausländischen Firmen unsere Zeugnisse überprüfen. Dann bestätigen wir denen die Echtheit, sofern eine Einverständniserklärung des Absolventen vorliegt.

Bei einer Bewerbung für ein Studienplatz an einer amerikanischen Universität bitten uns Absolventen darum, dass wir eine beglaubigte Kopie ihrer Abschlussunterlagen in einem gesiegelten Umschlag direkt an die Universität schicken.

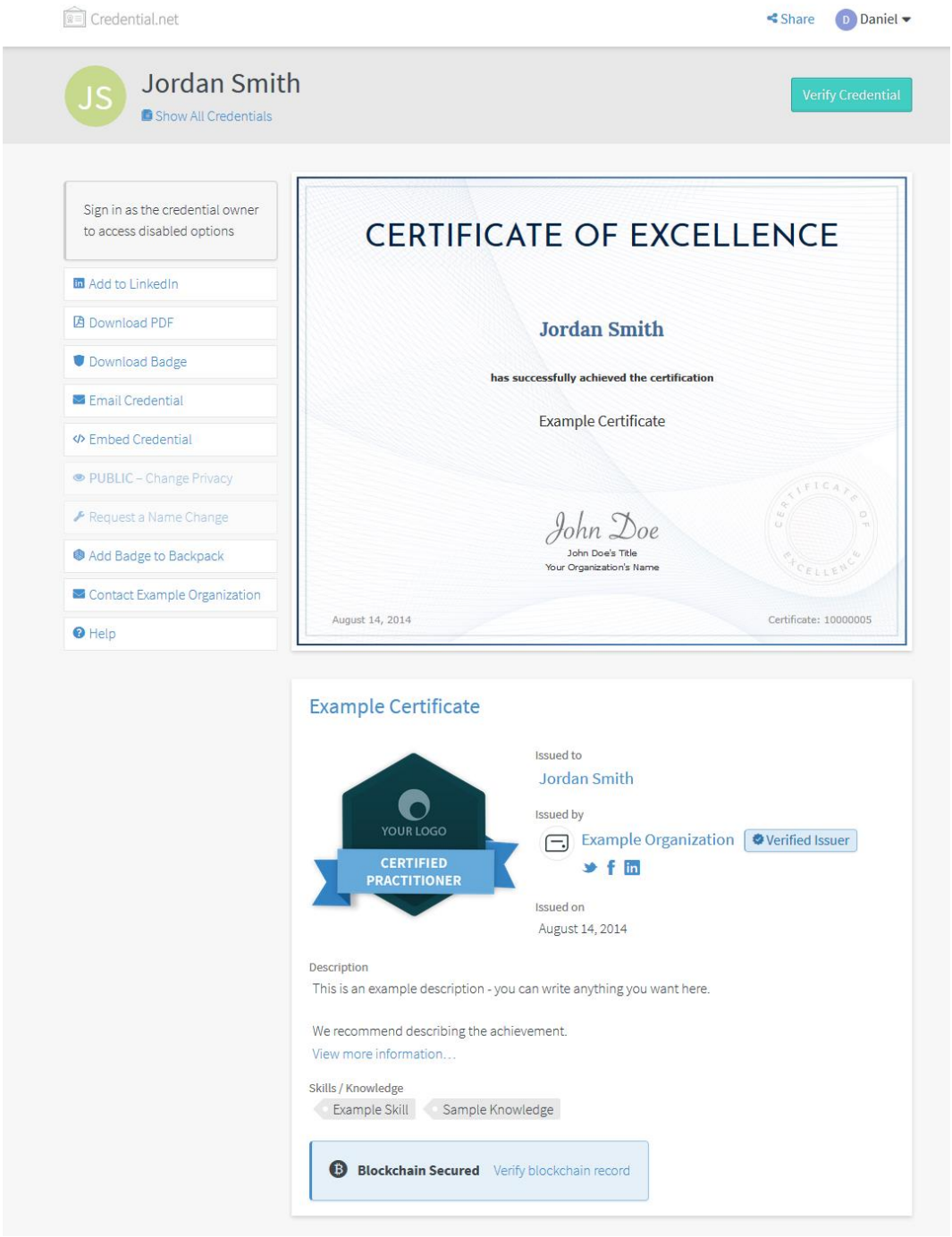
Ich hoffe, diese Auskünfte helfen Ihnen weiter.

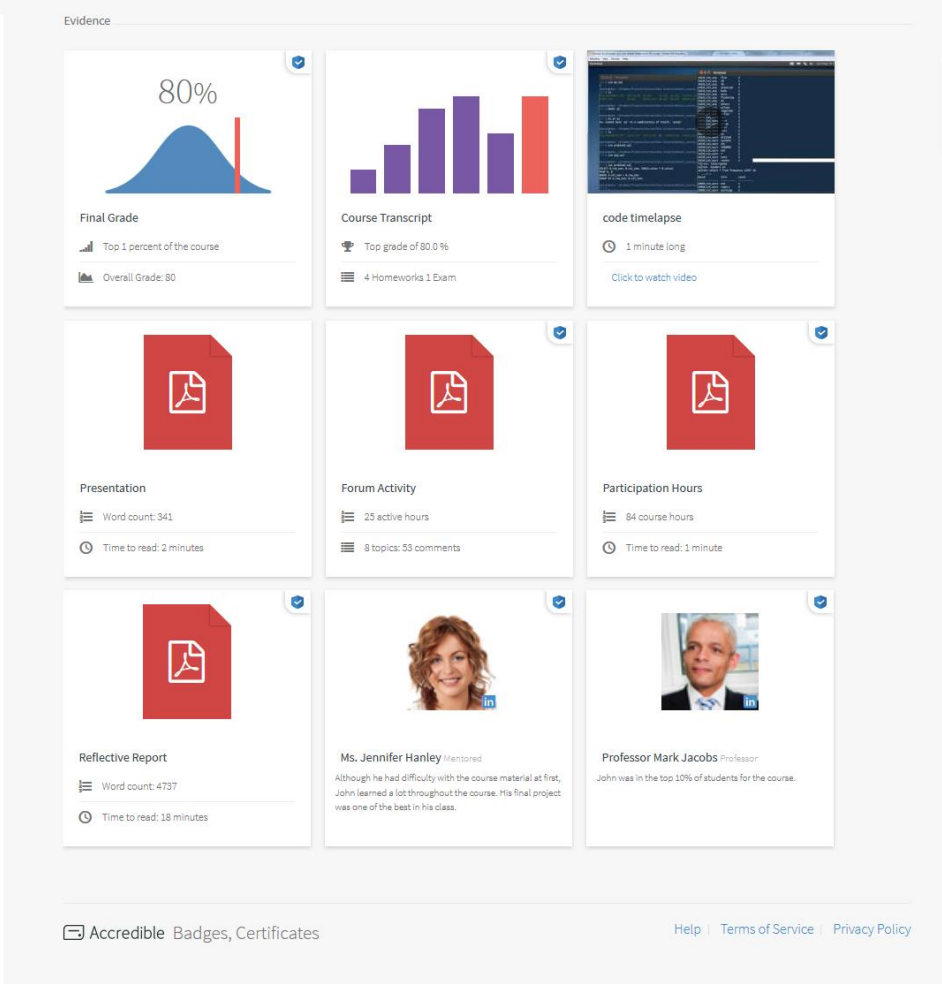
Mit freundlichen Grüßen
Claudia Hesse

Hochschulreferat Studium und Lehre T: +49 221-8275-5840 E: studium-suedstadt@th-koeln.de Technische Hochschule Köln Campus Südstadt Claudiusstraße 1 50678 Köln Räume: F1.41 und F1.41 a Postanschrift: Gustav-Heinemann-Ufer 54 50968 Köln Bitte beachten Sie unsere Öffnungszeiten und telefonischen Sprechzeiten: http://www.th-koeln.de/studienbuero-suedstadt www.th-koeln.de TH Köln Logo

Anhang 2: Accredible Screenshots und Beispiele

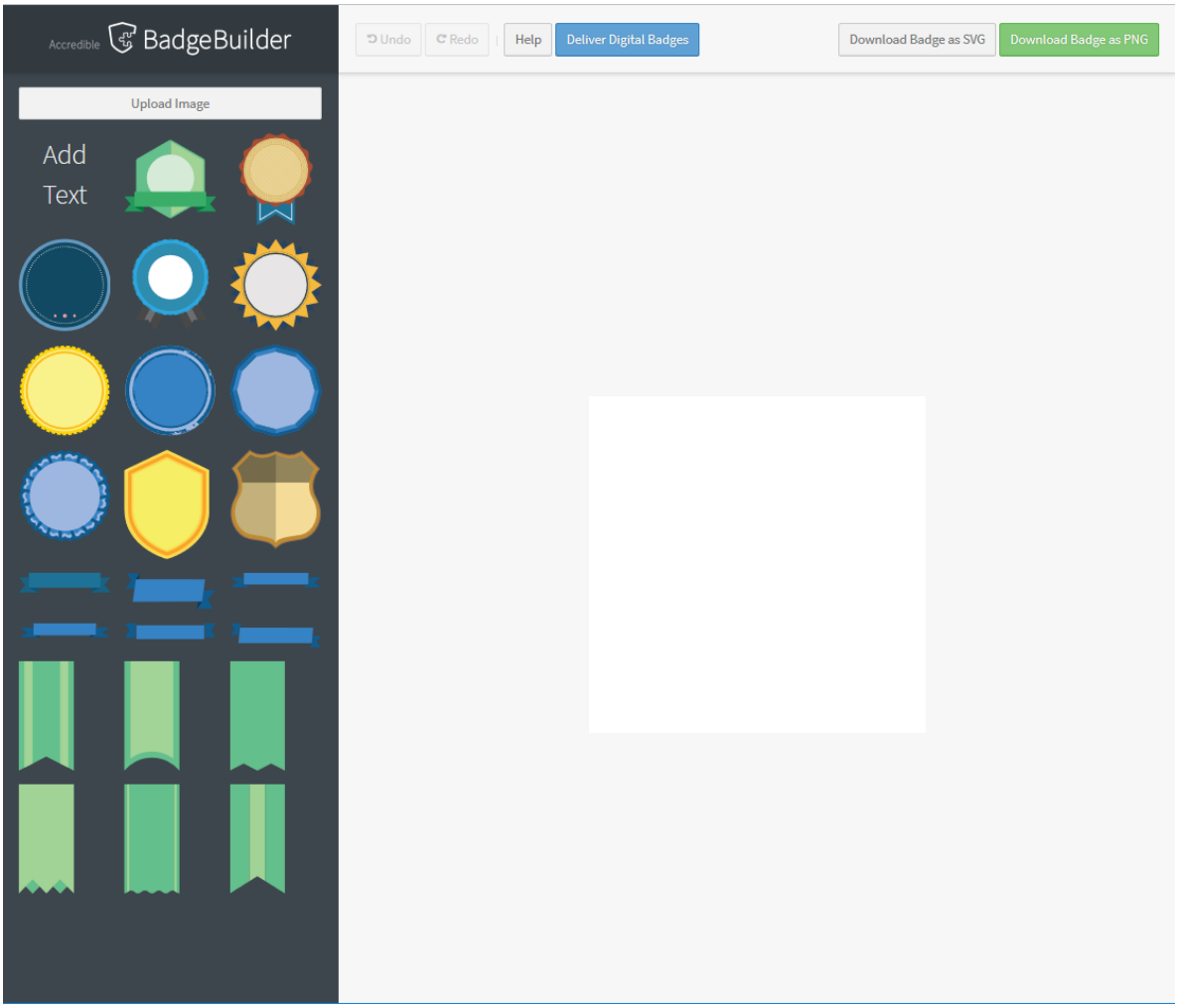
https://www.credential.net/10000005




Evidence
80%
Final Grade
Top 1 percent of the course
Overall Grade: 80
Course Transcript
Top grade of 80.0 %
4 Homeworks 1 Exam
code timelapse
1 minute long
Click to watch video
Presentation
Word count: 341
Time to read: 2 minutes
Forum Activity
25 active hours
8 topics: 53 comments
Participation Hours
84 course hours
Time to read: 1 minute
Reflective Report
Word count: 4737
Time to read: 18 minutes
Ms. Jennifer Hanley Mentored
Although he had difficulty with the course material at first, John learned a lot throughout the course. His final project was one of the best in his class.
Professor Mark Jacobs Professor
John was in the top 10% of students for the course.
Accredible Badges, Certificates
Help | Terms of Service | Privacy Policy

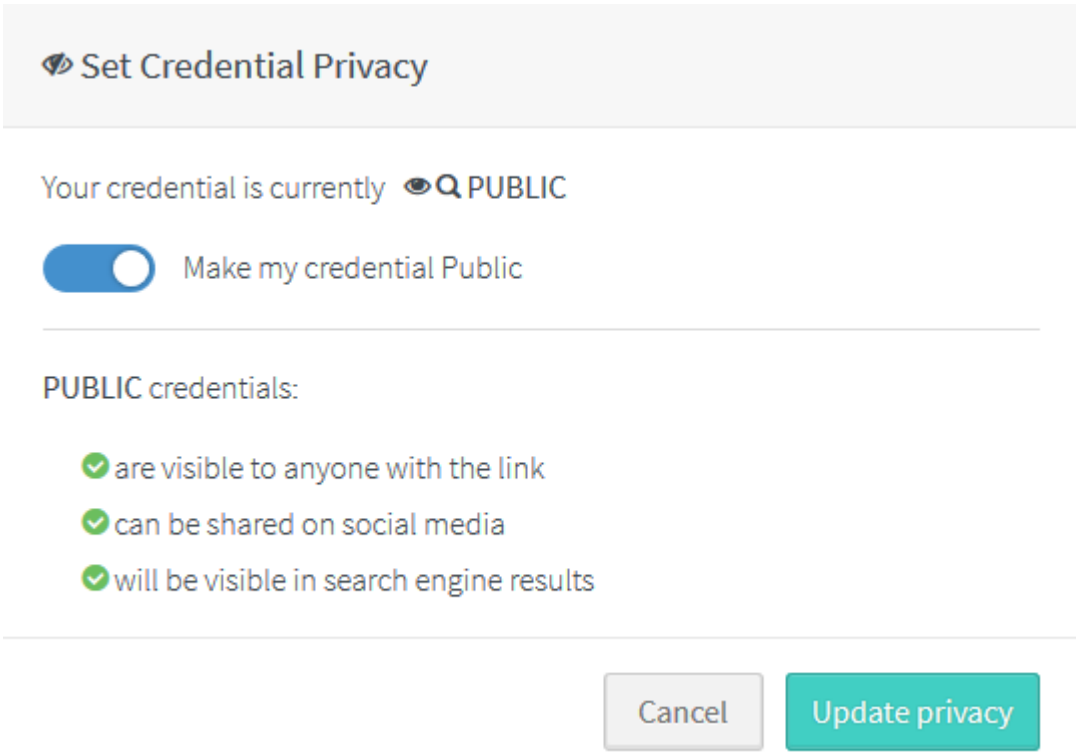
Accredible: Design-Editor

https://dashboard.accredible.com/issuer/dashboard/certificate_designs



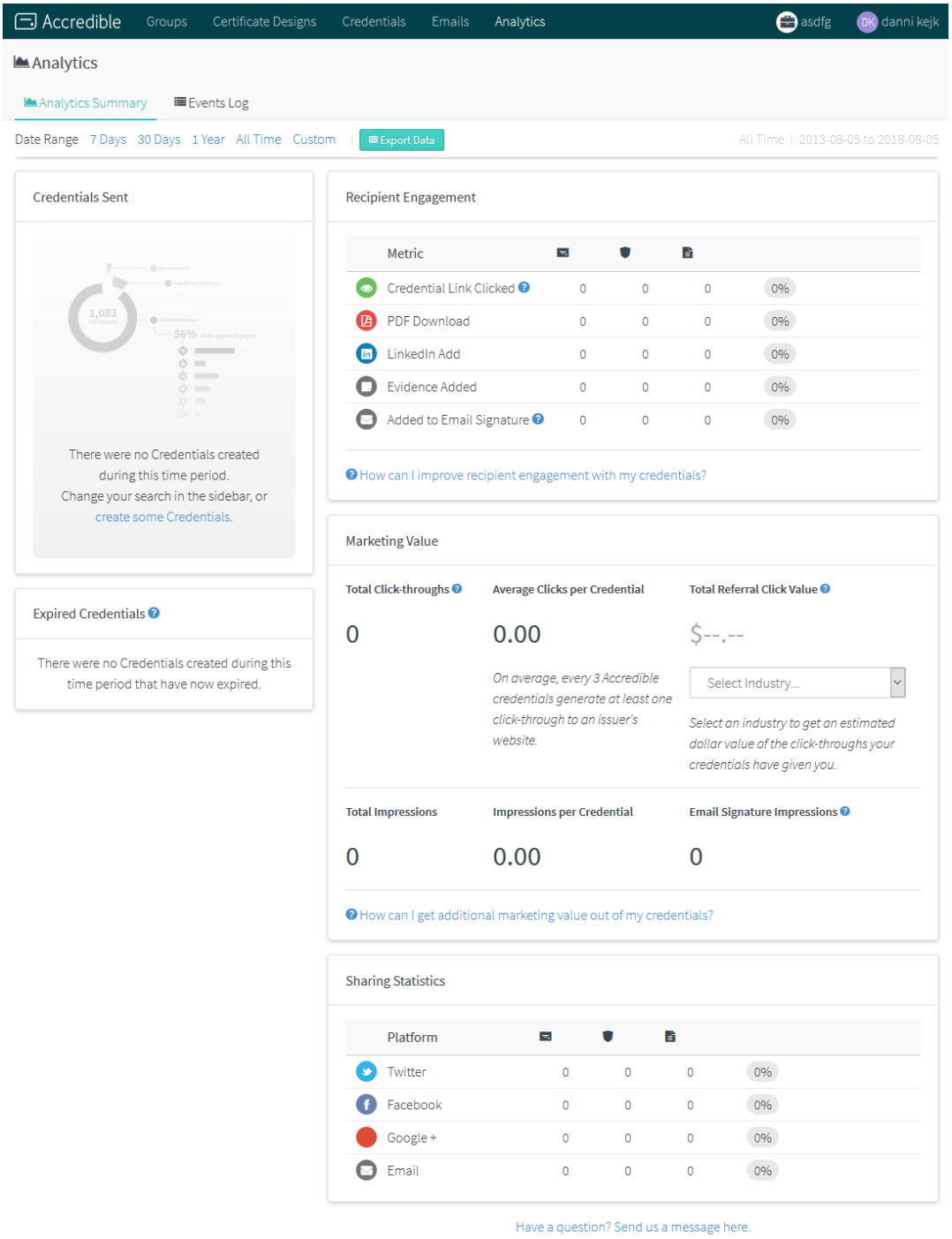
Accredible: Privatssphäre Optionen

https://www.credential.net/ep2zoffq



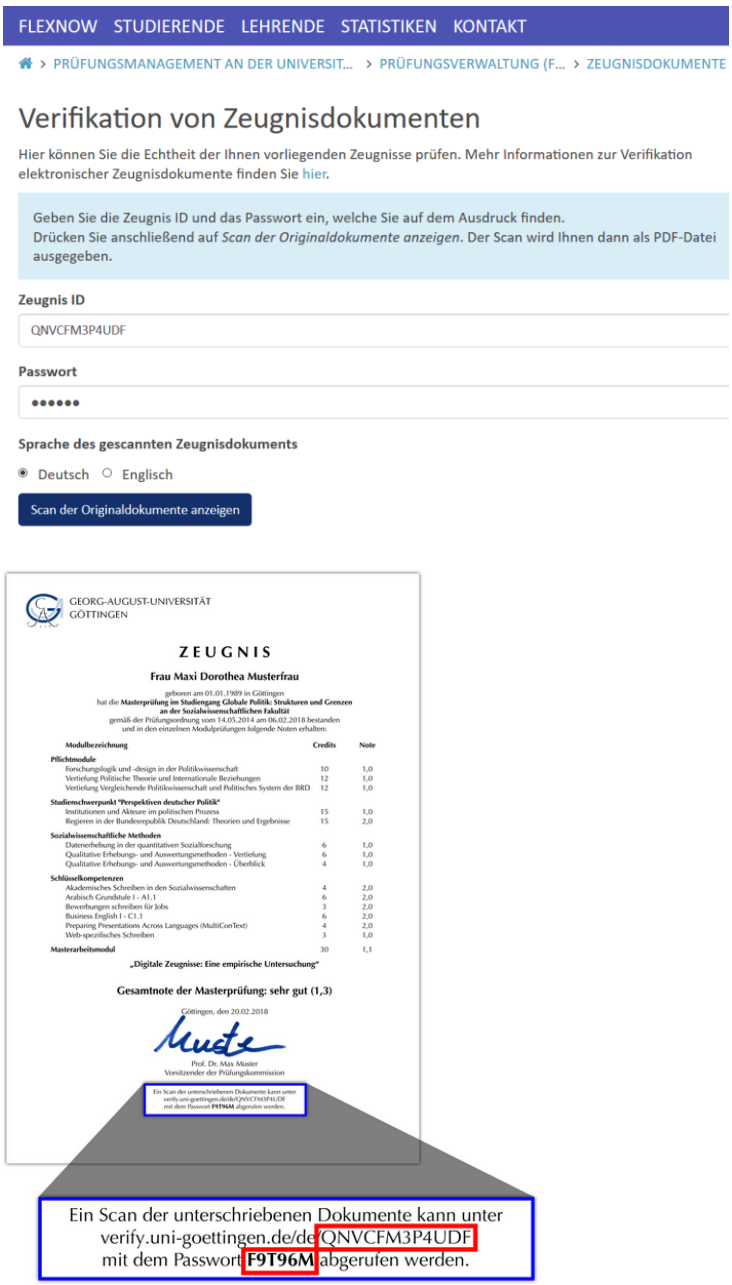
Accredible: Analytics

https://dashboard.accredible.com/issuer/dashboard/analytics/summary



Anhang 3: Digitale Zertifikate an der Universität Göttingen

https://www.uni-goettingen.de/de/574672.html?iframe_param={%22id%22:%22%22}



Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt wurde.

Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet. Dies gilt auch für Quellen aus eigenen Arbeiten.

Ich versichere, dass ich diese Arbeit oder nicht zitierte Teile daraus vorher nicht in einem anderen Prüfungsverfahren eingereicht habe.

Mir ist bekannt, dass meine Arbeit zum Zwecke eines Plagiatsabgleichs mittels einer Plagiatserkennungssoftware auf ungekennzeichnete Übernahme von fremdem geistigem Eigentum überprüft werden kann

Köln, den

_____

pers. Unterschrift